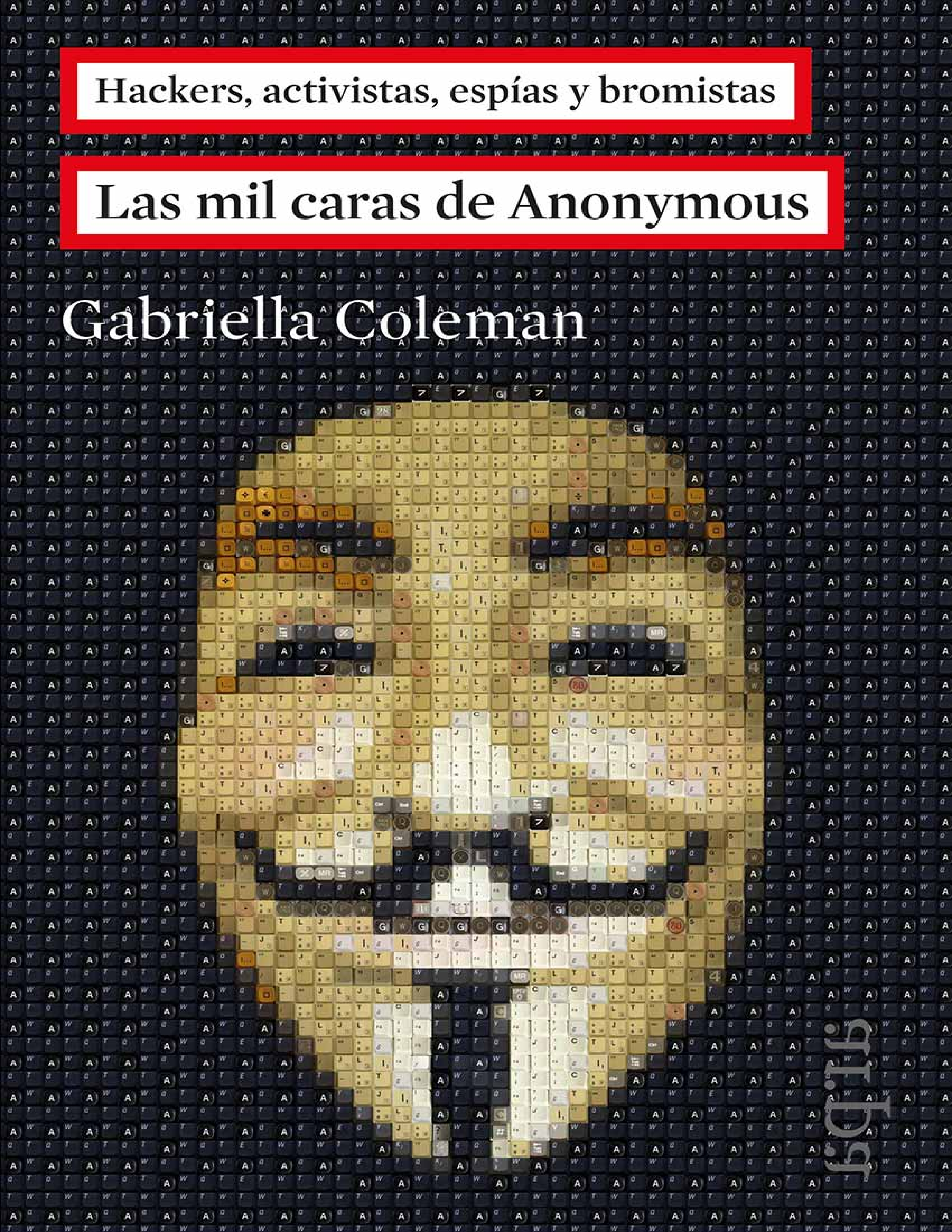


Hackers, activistas, espías y bromistas
Las mil caras de Anonymous
Gabriella Coleman

LAS MIL CARAS DE ANONYMOUS

Título original:
Hacker, Hoaxer, Whistleblower, Spy.
The Many Faces of Anonymous

Déu i Mata, 127, 1er – 08029 Barcelona
www.arpaeditores.com

Primera edición: febrero de 2016

ISBN: 978-84-16601-01-1
Depósito legal: B.549-2016

Diseño de cubierta y maquetación: Estudi Purpurink
Impresión y encuadernación: Cayfosa
Impreso en España / Printed in Spain

LAS MIL CARAS DE ANONYMOUS

Hackers, activistas, espías y bromistas

Gabriella Coleman

Traducción de Gerardo Di Masso

arpa editores

Este libro está dedicado a las legiones
que hay detrás de Anonymous:
a aquellos que han llevado la máscara en el pasado,
a aquellos que aún hoy se atreven a defender una postura,
y a aquellos que sin duda volverán a sublevarse en el futuro.

Índice

Introducción:

«Y ahora habéis captado nuestra atención»

El 29 de julio de 2007, una entidad autodenominada Anonymous —desconocida en aquel momento para todo el mundo excepto para los más eruditos cibernautas— colgó un vídeo en YouTube. En él, una nota musical digital, metálica, resuena mientras un hombre sin cabeza y vestido con traje aparece sobre un fondo blanco. Una voz masculina comienza a hablar a través de la interferencia: «Querida Fox News», entona la voz.[1] El programa de noticias había dedicado en fecha reciente un segmento completo a un grupo al que describía como «La Máquina del Odio de Internet», un título que el colectivo adoptaría posteriormente como lema honorífico.

Para un colectivo que disfruta con el engaño y la astucia, esbozar una simple sonrisa y desmentir semejante información pública hubiese significado perder una excelente oportunidad. Y por esa razón, la voz de Anonymous, grave e inquietantemente lenta y pesada, continúa: «El nombre y la naturaleza de Anonymous han sido devastados, como si se tratara de una prostituta en un callejón, y exhibidos luego ante la opinión pública. Permitidme que lo exprese de una manera muy simple: os habéis equivocado totalmente sobre quién y qué somos... Somos todos y no somos nadie... Somos el rostro del caos y los heraldos del juicio. Nos reímos ante la tragedia. Nos burlamos de los que sufren. Arruinamos las vidas de los demás simplemente porque podemos... Un hombre descarga su agresividad con un gato, nos reímos. Cientos de personas mueren en una catástrofe aérea, nos reímos. Somos la encarnación de una humanidad sin remordimiento, sin cariño, sin amor y sin sentido alguno de la moralidad.»

El vídeo concluye, «AHORA... HABÉIS CAPTADO... *NUESTRA* ATENCIÓN».

Ellos sin duda captaron la mía. Poco después de la publicación del vídeo, me vi inmersa en un proyecto de investigación de varios años sobre ese colectivo del que solo ahora he conseguido salir (este libro es la expresión monumental de esa lucha). El vídeo pretendía satirizar la caracterización hiperbólica que Fox News hacía de Anonymous como los máximos proveedores de bromas pesadas y troleo en Internet, «hackers chutados de esteroides», como les había denominado la Fox. Y, sin embargo, los sentimientos de miedo y el estilo escalofriante del vídeo plasmaron a la perfección el lado más aterrador de los trols. En lugar de desmentir el retrato ridículamente unidimensional de Fox News, el vídeo vino a confirmarlo plenamente, aunque solo, por supuesto, para aquellos que no estaban en el ajo.

Este doble significado refleja en una palabra el humor macabro de Anonymous (el lulz, lo llaman ellos). El lulz —un humor descarriado y un estado cuasi místico— ha evolucionado con Anonymous desde el principio, como veremos más adelante. Hubo un tiempo en el que difundir el caos del lulz era todo lo que parecía interesarle a Anonymous. Pero poco después de la aparición de este vídeo paródico y grandilocuente, Anonymous se hallaba en el centro de centenares de “operaciones” políticas, llegando a representar, incluso, una parte esencial de algunas de las luchas políticas más complejas de nuestra época. En solidaridad con los manifestantes tunecinos, en enero de 2011 Anonymous hackeó los sitios web del gobierno de Túnez; meses más tarde, el colectivo de indignados del 15-M español proyectó sobre un edificio de la Puerta del Sol la firma icónica colectiva representada por la máscara de Guy Fawkes; y miembros de Anonymous difundieron algunos de los primeros llamamientos a ocupar Wall Street.

Para entonces, el colectivo ya se había convertido en una fuerza política y social mediante una serie de operaciones que siguen siendo algunas de sus acciones más memorables. En 2008, partidarios de una nueva orientación para Anonymous desafiaron a la Iglesia de la Cienciología después de que la conflictiva organización intentase censurar un famoso vídeo grabado por Tom Cruise. Originados por la gracia de lulz, los Anons descubrieron tanto su poder para impactar en las luchas globales como el placer que esos compromisos podían reportarles. Dos años más tarde, en diciembre de 2010, Anonymous se hizo todavía más conocido a raíz de la “Operación Vengar a Assange”. Iniciada por AnonOps, uno de los

nodos más militante y prolífico del colectivo, muchos Anons participaron en una acción digital directa mediante una campaña de denegación de servicio distribuido (DDoS). Esta táctica, que interrumpe el acceso a las páginas web inundándolas con oleadas de solicitudes, iba dirigida contra las instituciones financieras que se habían negado a procesar las donaciones a WikiLeaks, incluidas PayPal y MasterCard. Con cada operación, Anonymous se envalentonaba aún más.

Aun así, incluso después de que Anonymous se alejase del incontrolable pandemonium de troleo para participar en la esfera política mundial, cada vez que la gente examinaba sus intervenciones activistas —ya fuese en una protesta callejera o a través de una intrusión informática de alto nivel— parecía surgir siempre la misma pregunta: ¿actúan Anonymous y sus partidarios disidentes impulsados por principios? ¿O se trata simplemente de unos críos que se dedican a joder en Internet como trols pasados de lulz?

Esta confusión es perfectamente comprensible. Más allá del compromiso fundacional de mantener el anonimato y de una generalizada dedicación al libre flujo de información, Anonymous carece de una filosofía consistente y de un programa político. Si bien se le reconoce cada vez más por su disidencia digital y su acción directa, Anonymous nunca ha exhibido una trayectoria previsible. Dado que la ascendencia de Anonymous se encuentra en el ocasionalmente humorístico, a menudo ofensivo y a veces profundamente invasivo mundo del troleo en Internet —cuya lógica básica parece ser, al menos a primera vista, un terreno inhóspito para el cultivo de sensibilidades comprometidas y empeños politizados—, resulta sorprendente que su nombre se convirtiese de entrada en un estandarte aprovechado por los activistas políticos.

Del troleo a los inadaptados del activismo

Cuando analizamos los orígenes de Anonymous, el amplio despliegue tanto de la máscara de Guy Fawkes —su principal seña de identidad— como de las ideas que acabó vehiculando entre los manifestantes de la Plaza Tahrir, en El Cairo, o de la Puerta del Sol, en Madrid, parece absurdo. Antes de 2008, el apodo Anonymous se utilizaba casi exclusivamente para definir

aquello que un Anon describe como *Internet motherfuckery* ("la mala leche de Internet"). Nacido en los foros del arbitrario tablón de imágenes /b/ de 4chan (considerado a menudo como "el retrete" o "el ano" de Internet), Anonymous era entonces sinónimo de trolear: una actividad cuyo objetivo es arruinar la reputación de personas y organizaciones y revelar información personal y embarazosa. Los trols tratan de amargarle la existencia a la gente mediante la difusión de contenido siniestro o perturbador, provocando polémicas o generando confusión. El caos suscitado por estos encendidos conflictos se puede generar usurpando identidades, creencias y valores simplemente por su potencial dañino, invadiendo foros en línea con spam o pidiendo centenares de pizzas, taxis e incluso equipos de los GEO para que acudan a un domicilio específico. Cualquiera que sea la técnica empleada, a los trols les gusta decir que hacen lo que hacen por el lulz, un animado pero a menudo malintencionado estilo de humor que deriva de LOL.*

Una de las primeras incursiones de troleo protagonizada por Anonymous —una acción épica hasta el día de hoy— colocó en el punto de mira a Habbo Hotel, una plataforma virtual cuyo eslogan reza efusivamente, «¡Haz amigos, únete a la diversión, hazte notar!». Pensada para adolescentes, esta plataforma finlandesa anima a los visitantes a crear avatares de lo más cursi, estilo Lego, que pueden relacionarse entre sí y personalizar las habitaciones del hotel con "furni"**. El 6 de julio de 2006, Anonymous se conectó al sitio de forma masiva, presentándose todos sus miembros como hombres negros vestidos con trajes grises y llamativos peinados afro. Al navegar de esa manera, fueron capaces de congregarse colectivamente formando esvásticas humanas y piquetes, impidiendo ambos que los miembros más asiduos de Habbo —principalmente niños—, pudieran acceder a la piscina del hotel. Cualquiera que intentase comprender la situación era informado por los personajes bigotudos de que la piscina estaba cerrada «debido a una avería y al SIDA».

Un par de años después de las primeras incursiones en Habbo, y apenas seis meses después de haber sido etiquetados como «la Máquina del Odio de Internet», algunos Anons comenzaron a utilizar el nombre y cierta iconografía asociada —en particular hombres sin cabeza vestidos con trajes negros— para coordinar protestas políticas. Esta sorprendente metamorfosis surgió de lo que muchos consideran una de las provocaciones más épicas de Anonymous: desafiar a la Iglesia de la Cienciología. «De un modo nunca

visto antes», destacó uno de los participantes en las incursiones, «la gran comunidad de Anonymous se unió para soltar una copiosa carga de “Que te jodan” sobre todo el imperio del culto de la Cienciología».[2] Impulsados por el lulz —por el deseo de liberar una avalancha de travesuras hilarantes y aterradoras— miles se subieron al tren del trol, bautizado “Proyecto Chanology”, para lanzar ataques DDoS a los sitios web de la Cienciología, encargar pizzas y prostitutas para iglesias de la Cienciología repartidas por toda Norteamérica, enviar por fax imágenes de partes de cuerpos desnudos a las iglesias e impulsar un aluvión de bromas telefónicas, especialmente dirigidas contra las líneas directas de la Dianética, destinadas a ofrecer consejos con respecto a «la primera tecnología realmente viable de la mente».

Al igual que había sucedido con la mayoría de las incursiones anteriores, muchos esperaban que este copioso “Que te jodan” seguiría su curso y se agotaría tras unos cuantos días de travesuras lúdicas y brutales. Pero un corto vídeo realizado por un pequeño grupo de participantes —creado solo para el lulz— provocó un serio debate en las bases de Anonymous. El citado vídeo “declaró la guerra” a la Iglesia: «Por el bien de vuestros seguidores, por el bien de la humanidad —y para nuestro propio entretenimiento— procederemos a expulsaros de Internet y desmantelaremos sistemáticamente la Iglesia de la Cienciología en su forma actual.»[3] Esta irónica declaración de guerra incitó a la gente a debatir y luego la catapultó a las calles. El 10 de febrero de 2008, más de siete mil personas en ١٢٧ ciudades se manifestaron protestando por los abusos contra los derechos humanos y los actos de censura practicados por la Iglesia de la Cienciología.

Por lo tanto, Anonymous pasó (según le explicó más tarde a mis alumnos un Anon participante) de las “cabronadas ultracoordinadas” a la difusión de hechos incriminatorios relacionados con la Cienciología. También forjó vínculos con una generación más vieja de disidentes que hacía tiempo que difundía los abusos cometidos por la Iglesia. El troleo había dado paso a un serio empeño activista, como si Anonymous hubiese emergido de su santuario en la red decidido a mejorar el mundo. Durante los dos años siguientes, algunos miembros de Anonymous apadrinarían a subgrupos de activistas ajenos y muchos participantes llegaron a identificarse como activistas de buena fe, si bien con un toque transgresor.

Muchas de las acciones protagonizadas por Anonymous, como la creación de vídeos publicitarios convertidos en una institución vernácula en sí mismos, son absolutamente legales. Pero hay un subconjunto de tácticas —especialmente los ataques DDoS y los hackeos— que son ilegales. Actos criminales bajo cualquier circunstancia, al menos en Estados Unidos. Los funcionarios del gobierno han realizado numerosos intentos de etiquetar sus actividades bajo el término genérico de "guerra informática" —para perseguir en consecuencia a sus participantes. El ejemplo perfecto de esta maniobra se dio el 21 de febrero de 2012, cuando el *Wall Street Journal* publicó que el general Keith Alexander, entonces director de la Agencia de Seguridad Nacional de Estados Unidos (NSA), había suministrado información a funcionarios de la Casa Blanca en el transcurso de reuniones secretas. El general Alexander afirmó que Anonymous «en uno o dos años podría tener la capacidad de provocar un apagón eléctrico limitado mediante un ciberataque».[4]

Mientras el artículo del *Wall Street Journal* rebotaba por las redes sociales, surgieron algunas preguntas. ¿Acaso esta afirmación le parece creíble a alguien? ¿Qué significa exactamente "capacidad" de provocar un apagón? De ser verdad esta afirmación, ¿cuál sería una respuesta apropiada? Es improbable que alguna vez lleguemos a saber si esa afirmación de la NSA se basaba en información fiable o si se trataba simplemente de ensuciar y desacreditar a Anonymous. En cualquier caso, la afirmación del general Alexander consiguió, al menos momentáneamente, presentar a Anonymous como una amenaza semejante a la de los yihadistas islámicos en la actualidad o a la del bloque comunista en tiempos pasados.

En última instancia, el mensaje no resultó convincente. Que se sepa, Anonymous, con todas sus diversas tácticas —tanto legales como ilegales, online y offline— nunca ha llamado públicamente a hacer semejante ataque. Y no existe ninguna prueba que sugiera que hayan contemplado esa idea. Poner en peligro vidas humanas nunca ha sido un tema de debate entre sus miembros, ni siquiera durante las más atropelladas conversaciones de salas de chat y foros. Las noticias posteriores citaban a activistas y expertos en seguridad que rechazaban las afirmaciones de la NSA, calificándolas de "información alarmista".[5]

A pesar de que una táctica de esta naturaleza sería absolutamente impropia de Anonymous, la relación del grupo con la opinión pública sigue

siendo ambivalente. Los métodos practicados por Anonymous son a veces subversivos, a menudo rencorosos, en general imprevisibles y con frecuencia desdeñosos de la etiqueta o la ley. Tomemos el ejemplo del "doxeo": la filtración de información privada —números de la Seguridad Social, direcciones particulares o fotografías personales— constituye un vacío legal, porque parte de la información revelada se puede encontrar en sitios web de acceso público.

En realidad, una sola operación de Anonymous puede integrar las tres modalidades —tácticas legales, ilegales y legalmente dudosas— y, si alguien tiene la oportunidad de incorporar el lulz a una operación, lo hará. Un ejemplo perfecto es la Operación BART, que se llevó a cabo en agosto de 2011. Anonymous entró en acción cuando los funcionarios del Distrito de Tránsito Rápido del Área de la Bahía de San Francisco (BART) intentaron desactivar la recepción de telefonía móvil en los andenes de la estaciones con el propósito de impedir una marcha convocada para protestar por la brutalidad policial. Los activistas locales habían convocado una manifestación de protesta contra el tiroteo que acabó con la vida de Charles Hill, un pasajero desarmado. Poco después, indignados por la intromisión de las autoridades en un acto de expresión democrática, algunos Anons ayudaron a organizar manifestaciones callejeras.

Un par de personas hackearon los ordenadores de BART y divulgaron datos de sus clientes con el fin de captar la atención de los medios de comunicación. Alguien encontró también una fotografía picante, en la que el portavoz oficial de BART, Linton Johnson, aparecía semidesnudo en su web personal. La foto fue reeditada en el sitio web "bartlulz" acompañada de esta impúdica reflexión: «si vas a ser un capullo con el público, seguro de que no te importará mostrarle la polla»***. En ocasiones tímidos y traviesos, a veces serios y estimulantes, a menudo todo a la vez (como la OpBART demostró perfectamente), aún a día de hoy estos activistas embaucadores están motivados por un anhelo colectivo de gamberradas y de lulz.

«Lo hice por el lulz»

¿Acaso la adopción permanente de la cultura de las travesuras en Internet,

del lulz, significa que llevar a cabo una investigación sobre Anonymous es un asunto alegre y desenfadado, la esencia de una diversión antropológica? Buscando información sobre la sorprendente metamorfosis de Anonymous —de inadaptados del troleo a inadaptados del activismo—, inicié en 2008 un estudio antropológico sobre el grupo. Al principio, mi investigación era sencilla, directa y ligera. Acudía a las protestas y seguía los debates en los foros virtuales y en Internet Relay Chat (IRC), una de las aplicaciones de comunicación más importantes para Anonymous (y muchos otros geeks y hackers).

En 2011, cuando Anonymous comenzó a desarrollar más tentáculos y los activistas pusieron en marcha docenas de operaciones políticas, este proyecto hasta entonces secundario se convirtió en mi vida. Durante más de dos años estuve permanentemente conectada online un mínimo de cinco horas diarias, luchando por mantenerme al día respecto de todas las operaciones que se llevaban a cabo de forma simultánea, algunas de las cuales se me ocultaban debido a su naturaleza clandestina. Investigar a Anonymous era como seguir un hilo a través de un sendero sinuoso y oscuro sembrado de rumores, mentiras, secretos y la macabra realidad de espías e informadores. El viaje ha estado marcado por vertiginosos estremecimientos, decepcionantes callejones sin salida y contorsiones morales, donde dilemas éticos en apariencia insolubles coexisten tranquilamente con ejemplos inequívocos de sacrificio y riesgo inspiradores. Más allá de las consecuencias derivadas de sus acciones, la propia estructura organizativa de Anonymous parecía igualmente intrincada y desconcertante. Con el tiempo algo quedó claro: Anonymous no era un simple laberinto, con una estructura y una ruta de escape que se revelaban a vista de pájaro; Anonymous era un laberinto mucho más complicado y enredado. No se trataba de un laberinto estático como el que Dédalo construyó en Creta para alojar al Minotauro. Era un mecanismo infinito que operaba un hermético bucle recurrente en el que los laberintos creaban laberintos que creaban laberintos.

A pesar de las dificultades a las que tuve que enfrentarme cuando atravesaba este laberinto, poco a poco llegué a conocer a Anonymous, y él a mí, en ocasiones a nivel personal. En mi calidad de antropóloga, observé, escuché, entrevisté, debatí, interrogué y presioné. En algunos momentos incluso participé, siempre que mi contribución fuese legal. Mis tareas eran

diversas: revisar manifiestos, enseñar a los periodistas cómo encontrar a Anonymous y corregir la información errónea.

Mi nivel de participación estaba limitado por barreras autoimpuestas y externas. El imperativo antropológico exige cierto grado de distancia, al tiempo que nos obliga a indagar en niveles más profundos. El truco consiste en integrar e ir más allá de la versión de los hechos que proporcionan los participantes. Yo simpatizaba con muchas de las causas y tácticas de Anonymous, pero no con todas ellas. Los dilemas morales de índole diversa creaban una distancia crítica. A causa de la naturaleza ilegal de algunas de sus actividades, determinadas áreas me estaban vedadas. Esto era mejor para Anonymous y para mí. Más tarde, después de los arrestos y las condenas, pude enterarme retrospectivamente de algunas acciones ocultas realizadas por el colectivo.

Con el predominio de las tácticas activistas en un nuevo grupo de Anons, hacia el verano de 2011, los desafíos cambiaron. Anonymous comenzó a desafiar a empresas de la lista Fortune 500 y a los contratistas militares en materia de defensa. Hackers mercenarios doxearon a Anons, revelando sus identidades a las autoridades policiales mediante la publicación de nombres legales, fotografías personales y domicilios. Algunos Anons empezaron a filtrar información sensible, clasificada o humillante. Entonces el FBI decidió intervenir. No importa cuánto lulz inyectase Anonymous en una operación: el humor no podía detener la propagación de un doloroso malestar entre los miembros y observadores del colectivo. De modo que, aunque a menudo mi investigación sobre Anonymous resultase emocionante, y sin duda siempre una aventura, a la larga hizo que me volviese paranoica.

Era una profunda sensación de paranoia, que planeaba sobre todas las cosas, como una perturbación barométrica antes de la llegada de un tornado. Me parecía justificada, pero quizá fuese por causa de la propia paranoia. Mientras llevaba a cabo mi investigación sobre Anonymous, tenía que mantener a los agentes de la ley alejados de mí y de mis datos. Cruzar una frontera representaba días de preparación para poner mis notas a buen recaudo y montar un ordenador de viaje seguro. El interrogatorio por parte de las autoridades siempre me parecía inminente. No me planteaba si los tíos del FBI me harían una visita, sino cuándo la harían. Me mantenía en guardia para proteger mis fuentes. Recordaba a los Anons que debían tener

cuidado con lo que me contaban. Nunca participaba en sus canales privados cuando planeaban operaciones ilegales.

A ojos del gobierno, yo me escondía estando a la vista de todos. No era una persona anónima en absoluto, esa era la ironía: pronunciaba conferencias sobre Anonymous, me entrevistaban periodistas continuamente y hablaba a menudo sobre Anonymous en programas de radio y televisión. En mi condición de profesora y académica de una importante universidad americana, era una persona fácil de localizar. En ocasiones, hasta altos ejecutivos de algunas de las empresas más poderosas del mundo se ponían en contacto conmigo, llamándome personalmente con la esperanza de que pudiese ofrecerles alguna información sobre un colectivo al que muchos de ellos habían llegado a temer.

Una pesadilla recurrente me persiguió durante años. Agentes del servicio secreto aporreaban mi puerta. Yo me despertaba súbitamente y me sentaba en la cama con el corazón desbocado: «Están aquí.» Era como *Poltergeist*, excepto que la cama no se sacudía y la posesión satánica desaparecía tan pronto como me sentaba sobre el revoltijo de sábanas.

Un día de 2012 despejé los restos de mi turbulento sueño con una taza de café bien cargado, dejando la pesadilla en un segundo plano para otro día. Con el cerebro plenamente en marcha caí en la cuenta de que ese día, 19 de abril, los papeles se invertirían: hoy sería yo quien llamaría a las puertas del Servicio de Inteligencia y Seguridad del Canadá (CSIS), el equivalente canadiense de la CIA. Con una mezcla de inquietud, ambivalencia y curiosidad, había aceptado la invitación del CSIS para dar una conferencia sobre Anonymous. Fui para descubrir qué era lo que el CSIS pensaba de Anonymous. ¿Los consideraban una amenaza terrorista, una banda de activistas alborotadores/fanáticos, o algo completamente distinto? Mi agenda secreta era comprobar su reacción al lulz: ¿podía una agencia responsable de la seguridad nacional llegar a percibir el humor de Anonymous? Para averiguarlo, preparé una simple prueba de fuego del lulz.

El cuartel general del CSIS se encuentra en las afueras de Ottawa, la capital de Canadá, instalado en un gran edificio de aspecto anodino, de color crema con detalles verde turquesa. Llegué sola, en taxi, abrumada por pensamientos en los que se mezclaban Orwell, *Brazil*, Huxley, Kafka y la vigilancia omnipresente de Bush/Obama. Me pregunté, «¿qué estoy haciendo aquí? ¿Qué acecha agazapado tras los muros de la agencia de

espionaje de Canadá? ¿Podía ser tan horrible como lo imaginaba? ¿Tiene esta gente salas de vigilancia de alta tecnología como en *Minority Report*? ¿Llevan a cabo experimentos psicológicos en salas de interrogatorio esterilizadas, revestidas de acero inoxidable*?*»

Mientras me ajustaba un traje de mujer de negocios que no me quedaba nada bien, me obligué a pensar que allí dentro encontraría aburridos cubículos de oficina con gente que hacía un trabajo rutinario y convocaba reuniones en monótonas salas de conferencias con teléfonos con altavoz en el centro de las mesas. Quizás en la puerta de la nevera de la sala de descanso había pegada una nota pasivo-agresiva porque alguien se había comido todos los timbits**** reservados para la fiesta de despedida que se celebraría más tarde. O encima del lavabo una nota manchada de agua con las palabras, «¡Tu madre no trabaja aquí, tendrás que limpiarlo tú!». Todo irá bien, me dije.

Para minimizar la angustia me había prometido que no les daría nada nuevo o secreto, me limitaría a hablar de lo que ya era de dominio público y donaría mis modestos honorarios a una asociación de defensa de las libertades civiles. Aunque había pronunciado esta misma conferencia docenas de veces, crucé la puerta principal sintiéndome aun más pequeña que mi figura de metro sesenta. Me recibió una mujer vestida con traje. A mi alrededor todo parecía absolutamente normal; no había nada siniestro a la vista, solo anodinas plantas de oficina.

Me llevaron a una sala con un pequeño escenario. La atmósfera era tensa. No alcanzaba a discernir la expresión en el rostro de ninguno de los presentes. Estaba casi paralizada de miedo. Entonces comenzó a preocuparme la posibilidad de que mi nerviosismo me hiciera decir algo que no debiera. Esos agentes, después de todo, estaban entrenados en el arte de extraer información; sin duda sabrían aprovechar cualquier oportunidad o muestra de debilidad para obtener ventaja. Con más de cuarenta personas mirándome fijamente, el ambiente de seriedad parecía quemarme a través del traje. No obstante, era algo que había hecho tantas veces que estaba en modo piloto automático y no fue hasta diez minutos después de haber empezado a hablar que me di cuenta que las manos me temblaban ligeramente, cuando intenté pulsar la tecla *play* de mi ordenador para activar la prueba de fuego del lulz: el famoso vídeo viral creado por Anonymous que había despertado su espíritu revolucionario. Cada vez que

había mostrado este vídeo en el pasado, tres frases en especial, sin excepción, habían provocado las risas de los presentes. ¿Se reirían a carcajadas los empleados del CSIS ante el lulz? En el vídeo, mientras las nubes se desplazan velozmente sobre un edificio corporativo acristalado, grande e indefinido, una voz dramática entona:

> Por lo tanto, Anonymous ha decidido que vuestra organización debe ser destruida. Por el bien de vuestros seguidores, por el bien de la humanidad y para nuestro propio entretenimiento. Procederemos a expulsaros de Internet y desmantelaremos sistemáticamente la Iglesia de la Cienciología en su forma actual.

La sala estalló en carcajadas. Misión cumplida; no existía mejor prueba del espíritu contagioso del lulz. Agentes de inteligencia riéndose de un vídeo realizado por trols de Anonymous, y precisamente de aquél que había dado origen a la "amenaza" que a ellos les encomendaron evaluar. «Saldré de aquí con vida, después de todo», suspiré en silencio.

Concluida la conferencia, un grupo más reducido de nosotros fue trasladado a una sala de reuniones estrecha y sórdida, sin ventanas, para tomar galletas y unos bocadillos insípidos bajo el intenso brillo de unos fluorescentes. Me pregunté si habría una sala más agradable, con claraboyas, reservada para los politólogos o los economistas y otros invitados mejor considerados. Nos acomodamos en las sillas e hicimos las presentaciones de rigor. Aún me sentía demasiado desubicada como para recordar cargos o funciones concretos, y mucho menos nombres. Desde luego, no tomaba notas ni grababa la conversación en secreto. Sospechaba que ellos sí. Que yo supiera, podía haber estado hablando con un grupo de conserjes o con funcionarios con acceso al máximo nivel de autorización de seguridad. Uno de los títulos, sin embargo, sí me llamó la atención: el de otro antropólogo que había en la sala. Cuando nos presentamos, asintió ligeramente y me sonrió. Yo, entretanto, hacía un gran esfuerzo para no alterar mi cara de póquer. En mi cabeza surgieron toda clase de preguntas: «¿Realmente se ha formado como antropólogo?, ¿A qué universidad fue?, ¿Quién dirigió su tesis doctoral?, ¿Cuándo y por qué decidió trabajar para el CSIS?, ¿Pagan mejor que en la Universidad?» Pero no las formulé. Me preocupaba que pudiese tomar mi curiosidad por un interés por trabajar para

el CSIS y quería evitar cualquier malentendido.

En el curso de lo que al principio pareció una conversación errática, finalmente resultó evidente la razón por la que me habían invitado. Querían saber una cosa concreta: si creía que Anonymous se había fijado como objetivo hacer caer la red eléctrica. El momento no era producto del azar. Apenas un mes antes, la NSA había declarado que Anonymous era una amenaza inminente para la seguridad nacional y supongo que Canadá sentía cierta presión internacional para vigilar a ese tenebroso grupo.

Contesté honestamente. Teniendo en cuenta todas las tácticas legales e ilegales desplegadas hasta la fecha, les expliqué, Anonymous nunca había reivindicado públicamente semejante ataque. En aquella época no había ninguna prueba que sugiriese que el grupo siquiera hubiese considerado llevar a cabo una acción de esa naturaleza. No creía estar divulgando ningún secreto, ya que había hecho declaraciones a la prensa sobre el mismo tema. De hecho, pensaba que le estaba haciendo un favor a Anonymous.

Naturalmente, como la profesora ocupada que era, no podía dedicar todo mi tiempo a visitar los numerosos canales de las diferentes redes de IRC, ni mucho menos a vigilar cada sala de chat donde pudiera desarrollarse semejante conversación. También había conversaciones privadas y canales solo por invitación expresa a los que nunca accedí. «Su sociología es laberíntica», expliqué expresamente, seguramente exhibiendo mis propias frustraciones en materia de navegación e investigación de Anonymous. Es probable que haya pasado más horas con la vista fija en la pantalla del ordenador y chateando con Anons que cualquier no-Anon, con la notable excepción de los informantes, que están obligados a permanecer conectados prácticamente a tiempo completo. Expliqué también que nunca había visto ni un atisbo de plan semejante. De hecho, cada acción radical, incluso el doxeo de policías agresivos, provocaba un debate polémico respecto de la idoneidad moral de esa acción. «Si bien Anonymous se muestra a menudo pernicioso y endiabladamente confuso —continué—, ciertamente su intención no es matar a nadie. Ellos se organizan en casa, posiblemente en zapatillas, tecleando locamente en el ordenador. Es probable que la única “violencia” en que algunos incurran sea virtual, durante las partidas de *World of Warcraft* al que seguro que juegan.» Para reafirmar mi posición decidí incluir un toque de humor, parafraseando a un

Anon que había difundido el siguiente chiste poco después de que la NSA afirmase que Anonymous era sin duda capaz de poner a la red eléctrica en jaque: «Así es, vamos a inutilizar la red eléctrica. Y sabremos que lo hemos logrado cuando todo el equipo que utilizamos para lanzar nuestra campaña quede completamente inservible.»

Las posturas se relajaron. Las risas volvieron a resonar entre los hombres del gobierno (y también las mujeres: al fin y al cabo estábamos en 2012). En mi opinión, todos parecían aliviados por mi evaluación de la situación. Ahora podían volver a centrarse en cuestiones más urgentes.

El chiste dio pie a otras conversaciones sobre el papel fundamental que desempeñaban los medios de comunicación en la amplificación del poder de Anonymous. Uno de los agentes del CSIS compartió su indignación hacia la prensa por convertir a este colectivo de colectivos en algo más poderoso de lo que debiera haber sido. Por mi parte, tengo que reconocerlo, saboreaba el hecho de que hombres del gobierno y Anons, enfrentados a cierto nivel, fueran sin embargo aliados (aunque superficialmente) en su actitud crítica hacia los medios de comunicación. En suma, todos estuvimos de acuerdo en que la prensa había contribuido a hacer de Anonymous lo que era hoy.

Entonces el antropólogo residente del CSIS, cuya área de especialización era el terrorismo en Oriente Medio, hizo un comentario improvisado que me sorprendió incluso a mí: los yihadistas, explicó, estaban impresionados por el nivel de atención que había conseguido Anonymous por parte de los medios. ¿Había oído correctamente?, me pregunté. No podía imaginar a los tíos de Al Qaeda o del Estado Islámico mirando los vídeos de Anonymous, y mucho menos entendiendo la naturaleza de su cultura o su política, especialmente el lulz. Pensaba que los yihadistas se sentirían ofendidos por las prácticas profanas, infieles y ofensivas de Anonymous. Con un coro de carcajadas, todos coincidimos en que lo más probable es que no celebrasen el lulz (y que careciesen por completo del mismo). La conversación me recordó algo que un Anon me había dicho durante una charla virtual informal:

<A>: sí, es esa idea del humor y la irreverencia lo que forma la base de esto [Anonymous]
<A>: es lo que hará que resulte imposible calificarlo como terrorista

A pesar de las risas, me seguía sintiendo bastante incómoda y era perfectamente consciente de mi máscara de desapego académico. A pesar de mi apariencia tranquila y compuesta, por dentro pensaba, «¡No puedo creer que esté bromeando sobre yihadistas, Anonymous y el lulz con el CSIS!» Solo quería largarme de allí, algo que finalmente hice al acabar el almuerzo. Sentí un profundo alivio cuando regresé al hotel. Y traté de alejar la acuciante idea de que mi habitación del hotel Lord Elgin, en el centro de Ottawa, reservada por el CSIS, estaba llena de micrófonos.

Todavía hoy no tengo del todo claro cómo me siento por haber visitado el CSIS. En esas situaciones, uno puede revelar información importante de manera absolutamente involuntaria, incluso cuando los agentes no estén buscando o preguntando nada en particular. Tal vez también haya algo poco ético en revelar lo importante que es la prensa en la difusión del poder de Anonymous. Es un poco como abrir el telón y desvelar que el mago es en realidad un viejecito que acciona las palancas de una máquina. Al mismo tiempo, el poder de los medios de comunicación es un secreto a voces dentro de Anonymous, una cuestión que los propios activistas debaten de forma rutinaria.

Visto en retrospectiva, y para bien o para mal, creo que hubo algo del espíritu embaucador que me empujó a aceptar la invitación del CSIS. Los embaucadores arquetípicos, como el dios Loki escandinavo, tienen un escaso control de sus impulsos; los guía la lujuria o la curiosidad. La curiosidad me impulsó a visitar el CSIS, a pesar de mi ansiedad y mis reservas. Necesitaba una respuesta a una pregunta apremiante: ¿se reirían con el lulz? De modo que supongo que, como los trols, «lo hice por el lulz». Por lo que vi en la agencia de espionaje de Canadá, obtuve mi respuesta: el lulz puede ser apreciado (casi) universalmente. Gracias al otro antropólogo que había en la sala, descubrí algo más. Esa broma final sobre los yihadistas y el lulz me enseñó otra lección sobre Anonymous que quisiera transmitir al comenzar esta aventura.

Ningún grupo ni persona puede reclamar la propiedad legal del nombre “Anonymous”, mucho menos sus iconos e imágenes. Naturalmente, esto ha contribuido a que Anonymous se extendiera por todo el planeta. Ahora se ha convertido en la “marca antimarca” por antonomasia, asumiendo diversos significados y configuraciones, y aunque también se

haya convertido en el rostro más popular de la agitación política alrededor del mundo. Aunque el nombre “Anonymous” es libre y gratuito —tal y como dijo Topiary, un activista de Anonymous, antes de ser arrestado: «No se puede arrestar una idea»—, el ejemplo de los yihadistas es un poderoso recordatorio de que su apertura radical no significa que cualquiera pueda o desee siquiera adoptar el nombre o las imágenes que lo acompañan. La cultura tiene una manera curiosa de afirmarse, incluso entre un grupo de activistas que buscan desafiar los límites y que han creado uno de los dominios de activismo más accesibles, resistentes y abiertos que existen de la actualidad.

De hecho, en el momento de mi visita al CSIS en 2012, Anonymous se había transformado en un colectivo multitudinario, prolífico e imprevisible. Por supuesto, como el colectivo es un subproducto de Internet, no debe sorprender a nadie que Anonymous se proyecte con mayor fuerza y reúna el mayor apoyo cuando defiende valores asociados con esta plataforma de comunicación global, como la libertad de expresión. Como lo definió en una ocasión uno de los participantes, «la libertad de expresión no es negociable». Pero lo que han demostrado una y otra vez es que no se limitan a mostrar su preocupación por las libertades civiles. Durante los últimos cinco años, los activistas han contribuido a una variedad realmente asombrosa de causas, desde la publicación de casos de violación (como en Halifax, Canadá, y Steubenville, Ohio), hasta prestar ayuda en las primaveras árabe y africana en 2011.

Varios son los factores que se confabulan para asegurar la flexibilidad del grupo. No existen mandatos acordados que deban mantenerse. Las personas asociadas con Anonymous resisten tenazmente la institucionalización. Su reputación es difícil de mancillar. Ni siquiera es necesario ser hacker (¡de veras!) para participar en las operaciones de Anonymous. La estética audaz del grupo, estilo Hollywood, toca una fibra familiar en nuestra sociedad del espectáculo. Y cuando Anonymous reacciona ante los acontecimientos que se producen en el mundo, participa en una amplia variedad de actividades, con las filtraciones y la exposición de las vulnerabilidades en la seguridad como dos de sus intervenciones más notables.

Todos estos elementos —que se entremezclan en diferentes proporciones y configuraciones—, hacen que resulte casi imposible saber

cuándo o por qué atacará Anonymous, cuándo aparecerá un nuevo nodo, si una campaña tendrá éxito y cómo podría el grupo cambiar de dirección o de tácticas en el curso de una operación. Quizá su carácter imprevisible sea lo que convierte a Anonymous en un colectivo tan temible para gobiernos y grandes empresas de todo el mundo.

Aunque endiabladamente difícil de estudiar, Anonymous no es del todo azaroso ni caótico sin más. Ser Anonymous significa seguir una serie de principios conexos. Anonymous está animado por un espíritu de desviación humorística, trabaja a través de diversos órganos técnicos (como el IRC), reposa sobre una ética antifamoseo e interviene políticamente de maneras asombrosamente ricas y variadas. Este libro intentará desentrañar algunas de las complejidades y paradojas inherentes a un Anonymous políticamente comprometido. Pero, antes de analizar sus intervenciones como activistas, examinemos con atención el siniestro submundo del troleo del cual eclosionó Anonymous.

Capítulo 1

Sobre trols, embaucadores y el lulz

Antes de 2008, cuando Anonymous reveló de manera inesperada una sensibilidad activista, la marca se había utilizado exclusivamente para aquello que, en la jerga de Internet, se conoce como "trolear": ir a por personas y organizaciones, profanar reputaciones y difundir información humillante. A pesar de la fama que Anonymous acumuló gracias a sus campañas de troleo masivo, desde luego no era el único jugador en ese campo. El panteón del troleo era entonces, y continúa siendo hoy, extenso y diverso. El troleo es una actividad variopinta que prospera en la red y ostenta un amplio abanico de asociaciones estrechamente unidas (tales como Patriotic Nigras, Bantown, Team Roomba o Rustle League), una variedad de géneros (diferenciados en su mayoría por el objetivo; por ejemplo, los *griefers* o "cibermatones" van a por jugadores de videojuegos; mientras que los RIP trols se centran en familiares y amigos de personas fallecidas recientemente) y un pequeño panteón de personas famosas (*Violentacrez, Jameth*). Su núcleo original se remonta mucho más allá de la creación de Internet y hunde sus raíces en las veleidades del mito y la cultura oral. A pesar de esta diversidad, los trols contemporáneos de Internet están unidos en una reivindicación casi universal del lulz como fuerza motriz y efecto deseado de sus esfuerzos. Nuestra historia puede empezar con uno de sus protagonistas más celebres.

Un día, de manera absolutamente inesperada, recibí una llamada telefónica de uno de los trols más famosos de todos los tiempos: Andrew Auernheimer, conocido simplemente como "weev". Se puso en contacto conmigo el 28 de agosto de 2010 mediante un mensaje telefónico que duró sesenta y dos segundos:

> Sí, Sra. Coleman. Soy weev. O sea W-E-E-V, y tal vez esté familiarizada con mi trabajo. Entiendo que prepara una presentación sobre hackers, trols y la política del espectáculo. Y solo quiero decirle que soy *el* amo del espectáculo. Éste es mi arte, señora. Y también ha dado una especie de conferencia sobre el lulz y yo estaba presente cuando se habló del lulz por

primera vez. Así que quiero asegurarme de que usted interpreta y representa correctamente mi cultura y a mi gente. No deseo que un charlatán cualquiera mienta sobre mi historia y mi cultura. De modo que quisiera hablar con usted y entender qué es lo que está haciendo y asegurarme de que no es solo otra profesora diciendo chorradas. Póngase en contacto conmigo, mi dirección de correo electrónico es gluttony@XXX.com. O sea G-L-U-T-T-O-N-Y en XXX punto com. Espero una respuesta, Sra. Coleman. Es *extremadamente* importante.

Después de escuchar el mensaje, mi sorpresa fue tan grande que dejé caer el teléfono. Estaba sobrecogida por la emoción, pero también por el miedo. Recogí el teléfono, pulsé rápido una secuencia de números interminable, volví a escuchar el mensaje tres veces más, lo grabé y regresé a casa de inmediato, solo para pasar el resto de la tarde con la cabeza llena de cábalas. Ojalá no hubiese llamado nunca.

La reputación de weev obviamente le precedía. Pese a mi rudimentaria investigación sobre los trols y la investigación en curso sobre el activismo de Anonymous, le había evitado como a la peste bubónica. Si bien el troleo se practica y disfraza a menudo como un juego, también está rodeado de misterio, peligro e imprudencias. Weev es ex presidente de uno de los grupos de troleo más exclusivos que existen en la actualidad, la ofensivamente denominada Gay Nigger Association of America (GNAA). (Sus afiliados ponen a prueba a los candidatos con preguntas triviales sobre una oscura película de ciencia ficción de serie B titulada *Gayniggers from Outer Space,* “Negratas maricones del espacio” en su versión en español, que inspiró el nombre del grupo.) Ponerse en contacto con un trol tan repugnante podría causar problemas. Los trols son famosos por llevar a cabo las llamadas campañas “arruina-vidas”, en las que difunden historias humillantes sobre una víctima (sin importar su veracidad) y filtran información personal, como direcciones particulares y números de la Seguridad Social. El efecto es semejante a ser maldecido, marcado y estigmatizado, todo a la vez. Los efectos psicológicos pueden ser aterradoramente duraderos.[6]

Pero como también corría un riesgo si decidía ignorar su petición —al fin y al cabo, él la había calificado de extremadamente importante—, le envié un correo electrónico unos días más tarde. Y puesto que ya me había lanzado al vacío, pensé que también podía tener sentido que me familiarizara con otro género de troleo. A diferencia del estilo presuntuoso, elitista y exhibicionista de weev, Anonymous había mostrado históricamente una modalidad de troleo mucho más modesta y populista. Como si fuesen las dos caras de una moneda, ambos

pertenecían a la misma “tribu” al tiempo que se oponían mutuamente. Durante un par de minutos incluso me planteé, con cierta emoción, detallar una tipología de los trols. Del mismo modo en que antaño mis ancestros antropólogos clasificaban tribus, cráneos y hachas, quizá yo podía hacer lo mismo con los trols y sus horribles proezas mientras, al mismo tiempo, también como ellos, jugaba con la tendencia histórica a la categorización irrelevante y, en ocasiones, racista. Pero mi entusiasmo se desvaneció rápidamente, cuando recordé la desastrosa realidad que esta decisión podía hacer caer sobre mí si me colocaba en el lado equivocado de estos trols famosos. Me acordé de que, por una muy buena razón, ya había tomado la decisión de centrarme en el activismo de Anonymous, no en el auge de su troleo. Al final, sencillamente esperé que weev ignorase mi correo.

Sin embargo, cuando respondió a mi correo electrónico comprendí que no tenía más alternativa que comprometerme. Acabamos conectando a través del chat de Skype. Su *handle* era “dirk diggler”, en referencia a la estrella porno protagonista en 1997 de la película *Boogie Nights*. Más tarde, cuando pasamos al IRC, utilizó “weev”:

<dirk diggler>: ¿cómo estás?
<biella>: bien, ¿y tú?
<dirk diggler>: recuperándome de los efectos de una vil sustancia
<biella>: te has levantado temprano
<dirk diggler>: metilendioxipirovalerona* creo que se llamaba
<dirk diggler>: es tarde, técnicamente
<dirk diggler>: dado que no he dormido
<biella>: yo me desperté a las tres de la mañana lo cual no es habitual en mí
<dirk diggler>: ahora mismo estoy trabajando en mi última tormenta de mierda
<dirk diggler>: los proyectos tecnológicos disruptivos son la hostia
<biella>: además eres un experto en eso
<dirk diggler>: sí estoy pasando de la mdpv al café
<dirk diggler>: espero que esto suavice el bajón el tiempo suficiente como para enviar este jodido mensaje en vivo hoy mismo
<biella>: no hay ninguna posibilidad de que estés en nyc en un futuro cercano, ¿verdad?
<dirk diggler>: probablemente no
<dirk diggler>: es una ciudad despreciable
<biella>: jaja, ¿de verdad?
<dirk diggler>: un lugar repugnante
<biella>: ¿cómo es eso?
<dirk diggler>: las únicas personas decentes en NYC son los israelitas negros
<dirk diggler>: nyc es una ciudad fundada por la repulsiva orden de los financieros

Su denuncia de “la repulsiva orden de los financieros” sonaba acertada,

considerando el reciente desastre financiero provocado por la imprudencia de esa gente, de modo que, pocos minutos después de haber iniciado mi primera conversación de buena fe con un trol de fama mundial, estaba de acuerdo con él:

<biella>: eso es verdad
<dirk diggler>: es un lugar pecaminoso y decadente
<biella>: cada vez hay menos espacio para los que no son ricos
<dirk diggler>: y dondequiera que las personas inmorales tienen el control, me doy cuenta de que todo el mundo quiere imitarles
<biella>: Detroit es como la única ciudad donde hay posibilidades en mi humilde opinión (gran ciudad)
<dirk diggler>: nah slab city es la que tiene más potencial en todos los EE.UU.
<dirk diggler>: una parte de god's war** se desarrolla allí en este momento
<biella>: nunca he estado allí

Es verdad: no había estado nunca en Slab City. De hecho, era la primera vez en mi vida que oía hablar de ese lugar. Y entonces, mientras chateábamos, busqué en Google "Slab City", que realmente existe y que es un fascinante refugio/campamento de okupas en el Salvaje Oeste, en California. Muy pronto aprendí que si bien weev miente con frecuencia, también dice la verdad a menudo, y su conocimiento de lo extraño, lo fantástico y lo siniestro es ciertamente enciclopédico. Weev es un etnógrafo nato de las expresiones más extremas e infames del esoterismo humano.

Al dedicar gran parte de su adolescencia y los primeros años de su edad adulta al hackeo y el troleo —y al consumo de ingentes cantidades de drogas, si le creemos—, weev había logrado reunir un enorme catálogo de hazañas técnicas y humanas. Su golpe más famoso, que le supuso una condena de tres años y medio en prisión, estuvo dirigido contra AT&T, un objetivo muy codiciado entre los hackers debido a sus cómodas prácticas de intercambio de información con el gobierno de Estados Unidos. (Las sobradamente conocidas actividades de AT&T en la habitación 641A, una instalación de interceptación de telecomunicaciones operada por la NSA, parecen pintorescas si tenemos en cuenta las noticias recientes de que la mayoría de los grandes proveedores de telecomunicaciones y de empresas de Internet facilitan al gobierno estadounidense un generoso acceso a los datos de sus clientes.) Weev fue a por AT&T a través de Goatse Security, el nombre elegido para el improvisado grupo de seguridad de GNAA. En junio de 2010 descubrieron que Telco, el gigante estadounidense, había hecho algo estúpido e irresponsable: los datos de los clientes de iPad de AT&T se habían publicado en Internet sin protección. Habitualmente, una empresa con buenas prácticas en materia de seguridad codificará cosas tales como los nombres de

clientes, las direcciones de correo electrónico y, por supuesto, los exclusivos números de identidad asociados a los iPads. Pero AT&T, al menos en este caso, no había codificado nada.

Aunque no dejaron los datos de los clientes en la puerta con un cartel colgado diciendo «Entren y cójanlos», acceder a ellos resultaba, no obstante, inusualmente sencillo. De hecho, Goatse Security descubrió una manera muy fácil de "sorber" los datos utilizando un *script* (un programa informático breve y fácil de aplicar) escrito por el miembro de GNAA/Goatse Daniel Spitler, alias *JacksonBrown*. El grupo de sombreros grises*** lo bautizó, con misteriosa precisión, el "Sorbedor de Cuentas iPad 3G", y lo utilizó para hacerse con los datos de 140.000 suscriptores. La oportunidad de dejar al descubierto un fallo de seguridad de tal magnitud resulta irresistible para cualquier hacker, incluso para uno como weev quien, como me contó durante la cena en la que finalmente nos conocimos en persona, ni siquiera tiene tanto talento tecnológico (o, como es más probable, sencillamente es demasiado perezoso para hacer el trabajo sucio, porque no cabe duda de que entiende muchos de los aspectos más técnicos relacionados con la seguridad).

En cualquier caso, Spitler escribió el *script* y desde entonces se ha declarado culpable ante los tribunales. Y weev también fue condenado en noviembre de 2012 por "hackear" el sistema de AT&T: una violación de la Ley de Abuso y Fraude Informático (conocida como CFAA). Pero el hecho sigue siendo que, puesto que no se podía hablar de seguridad alguna, técnicamente no había nada que "hackear." El *script* de Daniel Spitler no comprometía un sistema por otra parte seguro y weev —que contribuyó al *script* con pequeñas mejoras— actuó principalmente como publicista, ofreciendo la vulnerabilidad a los medios de comunicación de forma gratuita. Quería desenmascarar la asombrosa falta de seguridad de AT&T en beneficio del interés general y para potenciar su propio perfil público. Hay que señalar que la CFAA es un instrumento jurídico extremadamente potente, con atribuciones tan amplias que concede a la fiscalía un enorme poder en casi cualquier procedimiento jurídico que esté relacionado con la vaga noción de "acceso informático no autorizado". No tiene porqué tratarse de actividades de hacking. Algunos tribunales han interpretado que "acceso no autorizado" designa toda práctica informática que viole los términos y condiciones de uso u otras reglas fijadas por el dueño del ordenador.[7]

Después de su condena impuesta por la aplicación de la CFAA, el caso de weev concitó la atención de un trío de abogados de alto nivel: Orin Kerr, Marcia Hofmann y Tor Ekeland. Los abogados presentaron una apelación en el caso de weev con la intención de revocar lo que ellos, junto con muchos profesionales en

el ámbito de la seguridad, consideraban que constituía un peligroso precedente capaz de desanimar investigaciones futuras y vitales sobre cuestiones de seguridad. La industria de la seguridad emplea a hackers e investigadores que descubren las vulnerabilidades informáticas en las empresas, aplicando los mismos métodos que los ciberdelincuentes, con el fin de exponer los puntos débiles y fortalecer la infraestructura para beneficio tanto público como privado. Al final, en abril de 2014 —y solo después de que cumpliese aproximadamente un año de una condena a cuarenta y un meses de prisión—, su caso fue declarado nulo. Pero no debido a la parte de la apelación correspondiente a la CFAA, sino por una cuestión relacionada con la jurisdicción. El tribunal determinó que Nueva Jersey, donde se juzgó el caso, no era el estado donde se había cometido el delito. Tor Ekeland explicó la importancia de esta resolución judicial a *The Guardian*: «Si el tribunal hubiese fallado en sentido contrario, habríamos tenido una jurisdicción universal en... casos de fraude y abusos informáticos, y eso hubiese tenido enormes implicaciones para la legislación relativa a Internet y la informática.»[8] No obstante, aunque los partidarios de weev estaban encantados de verle en libertad y satisfechos de que las cuestiones sobre la jurisdicción se hubieran aclarado, muchos mostraban su decepción por el hecho de que los procedimientos dejaran intacta la cuestión más amplia de la CFAA; o sea, el precedente peligroso seguía vigente.

Al llevar esta información a los medios de comunicación, weev demostró que su intención iba más allá del simple troleo. Cualquier hacker que se precie pondría el grito en el cielo frente a un sistema de seguridad tan malo; llevar esa noticia a la prensa —lo cual genera forzosamente un enorme revuelo— puede ser una acción responsable. Por supuesto, al escuchar la historia en boca de weev quedaba claro que también lo había hecho por el lulz. Sonreía cada vez que aparecía el nombre de Goatse Security al mencionarse el incidente en las noticias. Imaginaba a millones de personas buscando en Google el extraño nombre de ese grupo de seguridad y luego retrocediendo horrorizadas ante la visión de una repugnante “supernova anal” brillando en sus pantallas.[9] Goatse es una imagen grotescamente famosa en Internet en la que aparece un hombre agachado y separándose las nalgas con las manos hasta un punto que nadie podría creer humanamente posible. Los que ven esta imagen ya nunca pueden olvidar lo que acaban de ver, no podrán olvidar ni siquiera el más mínimo detalle; sus mentes quedan chamuscadas por la imagen como si esas fauces abiertas, adornadas con un anillo, fuesen una marca de ganado al rojo vivo. La inmadurez de la broma hacía saltar las lágrimas de risa a weev, que se inclinaba sujetándose la barriga con ambas manos mientras sus hombros se sacudían y su risa sonaba como un

endiablado martillo neumático.

Era evidente que weev ofendía a todo el mundo, incluidos los agentes del orden. El testimonio definitivo de su naturaleza incendiaria quizá sea la sentencia un tanto dura emitida por el juez. Al fin y al cabo, weev ni siquiera había participado en la elaboración del *script*. La noche previa a su condena escribió en reddit, un popular sitio web nerd: «Lamento haber sido lo bastante amable como para darle a AT&T una oportunidad de reparar su error antes de entregar los datos a Gawker. La próxima vez no seré tan amable.»[10] Para justificar la condena, la fiscalía citó sus comentarios en reddit no una ni dos, sino tres veces.

Para weev, esa conducta incendiaria se ha convertido en una costumbre. Ha grabado discursos cargados de odio despotricando contra judíos y afroamericanos —“sermones”, los llama él—, colgados en YouTube. Son mensajes tan odiosos que incluso indignan a otros trols.

Comenzamos a chatear poco después de que empezaran sus problemas legales relacionados con AT&T. Durante los cinco meses siguientes chateamos con bastante frecuencia. Hubo momentos que solo pueden describirse como extraños. Tomemos, por ejemplo, una conversación que mantuvimos el 12 de diciembre de 2010:

<weev>: hola
<weev>: ¿cómo estás?
<biella>: bastante bien ¿y tú?
<weev>: no me puedo quejar
<weev>: GNAA ha cambiado las formas de gobernanza
<weev>: ahora es una democracia ateniense
<weev>: donde los que han completado su servicio militar
<weev>: es decir los que han hecho cualquier troleo guay
<weev>: ahora son aptos para votar sobre las medidas

Yo, lo recuerdo claramente, no lo podía creer. Pero aun así, conseguí teclear una respuesta a duras penas:

<biella>: ¿de verdad?

Entonces, de manera absolutamente inesperada, como sucede a menudo cuando uno chatea en Internet —especialmente con weev—, saltó a otro tema mientras yo escribía una respuesta sobre cuestiones de gobernanza:

<weev>: mi fiador me llamó inesperadamente
<biella>: ¿cómo era antes? [antes de convertirse en una democracia ateniense]

<weev>: sí
<weev>: sospecho que pueden arrestarme mañana o el 16
<weev>: tengo que separar las responsabilidades
<weev>: porque nadie puede hacer toda la mierda que hice yo
<biella>: ¿de verdad? [...]
<biella>: quiero decir, ¿por qué crees que van a arrestarte?
<weev>: mi fiador me llamó inesperadamente
<weev>: para comprobar mi dirección actual
<weev>: la última vez que pasó algo así
<weev>: al día siguiente echaron la puerta abajo a patadas

En aquel momento se encontraba bajo investigación. Ya sé que era un trol y todo eso, pero admitámoslo: la cárcel es una mierda. Le dije que iría a visitarle y le expresé mi solidaridad:

<weev>: gracias
<weev>: disfrutaré de la compañía
<biella>: y de los regalos sin gluten que llevaré conmigo
<weev>: :D
<weev>: acabo de descubrir
<weev>: cómo hacer un pan sin gluten aceptable
<weev>: solo tienes que usar una variedad de ingredientes
<weev>: arroz integral, tapioca y harina de teff
<weev>: y fécula de patata

Resultaba natural, pues, que weev, un trol sin gluten chateando con una antropóloga sin gluten, pasara sin problemas a una conversación sobre Pilates. Lamentablemente nunca obtuve una respuesta satisfactoria sobre la cuestión de la gobernanza trol. Muchas de nuestras conversaciones seguían este patrón imprevisible y divertido.

Por lo general yo era sincera con él, pero le seguía el juego a su autoproclamado papel de bromista. Al mismo tiempo, a veces no resistía la tentación de llamarle la atención sobre las mentiras que decía, incluso de trolearle un poquito:

<weev>: para ser un tío que abandonó el instituto tengo una gran variedad de conocimientos
<biella>: excepto que estudiaste antropología en la James Madison :-)
<weev>: sí bueno
<biella>: pero tienes una gran variedad de conocimientos
<weev>: no soy más que un pobre chico de pueblo de arkansas
<weev>: abandoné la universidad porque era demasiado para mi simple mente sureña
<weev>: además estaba asqueado por la degeneración de las instituciones americanas

<weev>: todas las ciencias sociales se habían convertido en un elaborado plan para infundir en los chicos blancos complejos de inferioridad racial o para destruir los roles de género que hacen que nuestra sociedad funcione

Como profesora en ciencias sociales tenía un conocimiento profundo de este "elaborado plan." No pude evitar alimentarle con algunas de mis propias mentiras:

<biella>: totalmente de acuerdo
<weev>: o si no promoviendo a los ideólogos judeo-bolcheviques/marxistas
<biella>: ellos nos forman en secreto para que hagamos eso (resulta bastante intenso)
<weev>: no sé si estás siendo sarcástica o sincera
<weev>: es la parte divertida
<biella>: lol
<biella>: bienvenido al mundo de biella chateando con weev :-)

De hecho, weev había pasado un tiempo en la cárcel de varios Estados hasta acabar en Nueva Jersey, donde fue puesto en libertad bajo fianza el 28 de febrero de 2011 a la espera de juicio. Puesto que ya no se le permitía utilizar Internet, nuestros chats se acabaron. En su lugar, continuamos nuestras conversaciones cara a cara, disfrutando de comidas sin gluten en Nueva York. Pagaba yo, ya que él estaba realmente sin blanca. Aunque weev me enseñó algunas cosas sobre el troleo, nunca utilizó sus habilidades conmigo.

A pesar de que las condiciones de la libertad condicional de weev le prohibían utilizar un ordenador, se las ingenió para seguir practicando su oficio. A weev, al igual que a muchos trols, le encanta engañar a la gente para llamar la atención. Estar en el punto de mira es una sensación genial, sobre todo si no tienes que pagar a un relaciones públicas para que cuelgue un vídeo sexual falso en la red. En mayo de 2011, con el verano llegando a Nueva York, me envió un mensaje de texto. «Busca mi nombre en Google», escribió. Hice lo que me pedía y en mi navegador aparecieron cientos de nuevos artículos. Había conseguido engañar a los medios de comunicación con un montaje presencial, afirmando que era vecino de Dominique Strauss-Kahn inmediatamente después de que se presentaran cargos por violación contra el acaudalado político francés y exdirector del Fondo Monetario Internacional. Weev, entonces en la indigencia absoluta, consiguió colar sus comentarios en centenares de periódicos y ningún periodista se molestó en verificar los hechos:

> A pesar de las alegaciones de la fiscalía, Strauss-Kahn ya está conociendo a sus vecinos. Un infame hacker informático que vive en el edificio de

apartamentos corporativo en Broadway afirma que ya ha conocido al francés y que es “un tipo legal”.

«Allí somos como un gran *Breakfast Club*», señaló Andrew Auernheimer, de 26 años, en referencia al film clásico de 1985 sobre cinco estudiantes de instituto que deben pasar el sábado en el colegio cumpliendo un castigo.[11]

EN EL LULZ CONFIAMOS

De modo que si weev, como tantos trols, sirve sus acciones en bandejas combinadas de verdades y mentiras, ¿es posible determinar si se encontraba realmente en la habitación cuando el “lulz” fue pronunciado por primera vez? Para investigar un poco más esta cuestión acudamos a la Encyclopedia Dramatica (ED), un compendio virtual increíblemente detallado que cataloga la mecánica, historia, gore y tradición trol. A pesar de ostentar el título de “Enciclopedia”, no ofrece ni neutralidad ni objetividad. Sin duda, la ED es una obra enciclopédica por su nivel de detalle, pero su tono resulta escandaloso y está plagada de mentiras. Lo que la ED hace bien (logrando de esta manera una extraña dosis de objetividad), es exhibir la cinética moral del troleo. Así pues, ¿la etimología del lulz que ofrece la ED, un fragmento de la cual se muestra a continuación, es fábula o realidad?:

> LULZ es una corrupción de L O L, que significa “reírse a carcajadas”, reírse a costa de otra persona. Esto la convierte en una expresión inherentemente superior a otras formas de humor inferiores. Anonymous consigue un gran lulz haciendo bromas pesadas indiscriminadas. Estas bromas pesadas se cuelgan siempre en Internet. Así como el elemento sorpresa transforma el acto físico del amor en algo hermoso, la angustia de la víctima de una broma pesada transforma el lol en lulz, haciendo que la risa sea más larga, gruesa y placentera. El lulz es utilizado por internautas que han presenciado demasiadas veces desastres económicos, ambientales o políticos importantes y que, por consiguiente, consideran que un estado de sociopatía voluntaria y alegre respecto del estado apocalíptico actual del mundo es algo superior a ser continuamente emo****.
>
> El término “lulz” fue acuñado por Jameth, un administrador original de la Encyclopedia Dramatica, y alcanzó una gran popularidad en ese sitio. El

> vocablo apareció a comienzos de 2001 mientras James (su verdadero nombre, siendo el sufijo -th un juego de palabras respecto de su homosexualidad y su pequeño pene) estaba manteniendo una conversación con un homosexual que ceceaba. A James se le llamaba *Jameth* por el defecto de habla de ese tipo. En junio de 2001, James decidió utilizar *Jameth* en su nombre de cuenta del LiveJournal. No dejes que te engañe, a James le encanta la polla.[12]

Según la información recogida en múltiples entrevistas, incluida una con el agudo e ingenioso fundador de la ED, Sherrod DeGrippo, weev participó efectivamente en la conferencia telefónica durante la cual Jameth acuñó el término. Y Jameth es, de hecho, gay. Nunca he preguntado por su ceceo.[13]

Actualmente el lulz también incluye bromas ligeras, utilizadas y disfrutadas por muchos nerds de Internet del mundo entero. Pero, inicialmente, fue concebido como algo cruel; a los trols les gusta definirlo como «reírse a costa de la desgracia de los demás.» El lulz es un ejemplo perfecto de lo que los folcloristas definen como argot, una terminología especializada y esotérica empleada por un grupo o subcultura. Como el argot es algo muy opaco y particular, funciona para generar secretismo o, como mínimo, erigir barreras sociales muy rígidas. Como antropóloga, por muy ridículo que pueda parecer, resulta tentador examinar el lulz en clave epistemológica, mediante la producción social del conocimiento. A un determinado nivel, el lulz funciona como un objeto epistémico, estabilizando un conjunto de experiencias y consiguiendo que sean aptas para la reflexión. Durante décadas no existió ningún término para definir el lulz, aunque trols y hackers experimentasen los placeres característicos derivados de las bromas pesadas en Internet. Una vez que un nombre como "lulz" ve la luz, favorece la práctica misma que nombra y la somete a una nueva reflexión por parte de sus practicantes. Los trols pontifican ahora sobre el significado del lulz, empleando el término para designar actos especialmente gratificantes (hayan o no sido producidos intencionadamente para el lulz), y también para diagnosticar situaciones que carecen de lulz y que, naturalmente, exigen cursos de acción reparadores.

¿Qué hace o significa ese término que ninguna otra palabra pueda captar? Es difícil de explicar. Pero si tenemos en cuenta que lulz deriva del acrónimo "lol" (reírse a carcajadas), es evidente que trata fundamentalmente de humor. Los lols son familiares a cualquiera que haya enviado alguna vez una broma por correo electrónico. Los lulz son más oscuros: practicados casi siempre a expensas de alguien, propensos a errar el tiro y, ocasionalmente, al límite del lenguaje odioso

o inquietante (excepto, por supuesto, cuando se pasan totalmente de la raya: bromas sobre violaciones no, gracias). Los lulz están inconfundiblemente imbuidos de peligro y misterio y, en consecuencia, tratan primordialmente de los placeres derivados de la transgresión.

Los rasgos definitorios del lulz son visibles en el *affaire* de weev con AT&T, no por la exposición de una brecha de seguridad sino por la manera en que consiguió que respetables comunicadores a lo largo y ancho de los Estados Unidos pronunciaran la palabra “Goatse”, refiriéndose involuntariamente a una de las imágenes más repugnantes que se pueden encontrar en Internet. En la práctica, las actividades lúlzicas desafían cualquier barrera pero también las vuelven a erigir. Existe una línea divisoria clara entre la gente que simplemente LOLea en Internet —sin saber realmente qué es Internet o de dónde viene o cómo funciona por dentro—, y aquellos que lulzean (es decir, hackers, trols, etc.), y que saben exactamente de qué trata el asunto. Los lulz son tanto una forma de diferenciación cultural como una herramienta o arma utilizada para atacar, humillar y difamar a los LOLeros normales involuntarios, a menudo incluso sin que se den cuenta de que existe toda una cultura alineada contra ellos. Habitualmente, los lulz son bromas privadas, pero (con frecuencia) pueden estar abiertas a los demás, provocando carcajadas no solo entre trols, sino también entre los demás. El peaje de la admisión es solo un poco de conocimiento. Los LOLeros pueden ser atraídos hacia el mundo del lulz gracias a sitios web habitados por trols como Encyclopedia Dramatica, 4chan y Something Awful, que se encargan de difundir este conocimiento a cualquiera que se ocupe de buscarlo. Las personas que lo encuentran pueden elegir entre alejarse rápidamente o convertirse en la siguiente generación de trols.

El lulz muestra con qué facilidad y casualidad los trols pueden poner patas arriba nuestro sentido de la seguridad a través de la invasión de espacios privados y la exposición de información confidencial. Las víctimas elegidas reciben en casa montones de pizzas sin pagar o ven cómo se publican sus números telefónicos no listados, se filtran sus números de la Seguridad Social, se cuelgan en la red sus comunicaciones privadas, se doxean los números de sus tarjetas de crédito y se siembra el contenido de sus discos duros. Los trols disfrutan profanando cualquier cosa remotamente sagrada, tal como lo define la teórica cultural Whitney Phillips en su astuta caracterización de los trols como «agentes de digestión cultural [que] hurgan como carroñeros en el paisaje, modifican el material más ofensivo y luego escupen las monstruosidades resultantes a la cara de una población desprevenida».[14]En resumen: cualquier información que se considere personal, segura o sagrada constituye un objetivo prioritario a

compartir o profanar de múltiples maneras. Las acciones orientadas hacia el lulz hacen añicos el consenso que rodea nuestra política y nuestra ética, nuestras vidas sociales y nuestras sensibilidades estéticas. Cualquier presunción de la inviolabilidad de nuestro mundo se convierte para ellos en un arma; los trols invaden ese mundo señalando la posibilidad de que los geeks de Internet lo destruyan, de dejarnos indefensos cuando sientan la necesidad de hacerlo.

Llegué a los trols justo en el momento en el que un subgrupo estaba experimentando una transformación crucial: cada vez más, la gente que trabajaba bajo la égida de Anonymous comenzaba a dedicarse al activismo. Considerando el sórdido panorama de vulnerabilidad que acabo de describir, esta evolución no podía sorprender a nadie. Sin embargo, no carecía de un precedente histórico: reconocí a los trols como parientes de los arquetipos del embaucador presentes en los mitos. Después de todo, soy antropóloga y los embaucadores son un tema ancestral de la reflexión antropológica.

¿Broma o regalo?

El arquetipo del embaucador se presenta plagado de un gran número de iconos y relatos a menudo encantadores. Las mitologías griega y romana aportaron algunas de estas figuras al corazón de la cultura occidental: el Hermes mercurial y el beodo Dionisio, entre otros. En los folclores de África occidental y el Caribe este papel recae en Anansi, una araña que, a veces, imparte conocimientos o sabiduría y, otras, arroja dudas o siembra la confusión. Eshu, el dios de la comunicación y las encrucijadas en la cultura yoruba, es una deidad igualmente ambigua. Conocido por organizar escenarios caóticos que fuerzan las decisiones humanas, puede ser un maestro amable o un agente de la destrucción. Entre los indígenas norteamericanos, el Cuervo inicia el cambio por voluntad o accidente, y el Coyote es una bestia egoísta que engañará a cualquier criatura —humana o animal— para satisfacer sus apetitos. Desde la época medieval, la concepción occidental del embaucador se ha transmitido a menudo a través de la literatura. Puck, «el espíritu astuto y vil» que «engaña a los descarriados de la noche, riéndose de su dolor» en *Sueño de una noche de verano*, no fue una invención de Shakespeare sino que hunde sus raíces en una traviesa fábula del folklore celta. El metamorfo Loki de la mitología escandinava ha reaparecido recientemente en películas y series de Hollywood, principalmente como una versión insulsa de su ser mitológico, y sigue actuando como un recordatorio del papel caprichoso y vengativo que puede desempeñar el embaucador.

Los embaucadores están unidos por unas pocas características, tales como el deseo ardiente de desafiar o contaminar reglas, normas y leyes. A menudo carecen tanto del control de los impulsos como de la capacidad de experimentar vergüenza alguna, son descarados y su discurso no tiene ningún filtro. Algunos embaucadores están impulsados por una llamada superior, como es el caso de Loki, quien en ocasiones trabaja para los dioses (aunque fiel a su naturaleza temible acostumbra también causarles problemas). A muchos les motiva la curiosidad y un apetito voraz. Raramente planifican sus acciones, eligiendo en cambio una espontaneidad desenfrenada que se traduce en una artera imprevisibilidad. Si bien el capricho suscribe a menudo las exitosas proezas del embaucador, también puede causar tropiezos a los trols.[15]

Los relatos sobre embaucadores no son didácticos ni moralizantes sino que exhiben sus lecciones de un modo lúdico. Pueden funcionar normativamente —cuando los padres cuentan historias aterradoras para disuadir a sus hijos de que se comporten mal— o críticamente, permitiendo que las normas se pongan en evidencia para someterlas al reto folclórico-filosófico. Lewis Hyde, quien ha escrito extensamente sobre el tema del embaucador, observa que «los orígenes, la animación y la duración de las culturas requieren que haya un espacio para aquellas figuras cuyas función consiste en revelar y perturbar precisamente aquellos elementos en los que se basan las culturas».[16]

No resulta difícil imaginar al trol y a Anonymous como figuras embaucadoras contemporáneas. Son provocadores y saboteadores que desmantelan la convención al tiempo que ocupan una zona límite. Están bien posicionados para impartir lecciones, independientemente de su intencionalidad. No es necesario que sus acciones sean aceptadas, ni mucho menos avaladas, para extraer un valor positivo de ellas. Podemos verles como edificándonos con perspectivas liberadoras o aterradoras, como síntomas de problemas subyacentes que merecen ser examinados, actuando como una fuerza positiva orientada hacia la renovación, o como sombras deformantes y confusas. El embaucador se convierte en heurístico —no precisamente el único o el principal— para entender las fuentes, la multiplicidad de efectos y, especialmente, las dos caras de entidades moralmente inasibles como los trols y Anonymous.

Antes de llegar propiamente a Anonymous, merece la pena hacer un recorrido breve (incompleto) por la vibrante tradición del troleo/embaucamiento en Internet. La naturaleza de Internet —una red basada en el *software*— lo convierte en una herramienta ideal tanto para el juego como para la explotación;[17] es como un laboratorio para las travesuras. De hecho, los hackers (y más tarde los trols) han frecuentado este tipo de comportamiento durante mucho tiempo. Pero

sólo recientemente algunas de estas actividades han alcanzado un estatus mitológico más visible y públicamente disponible. Por ejemplo, reunidos en la Encyclopedia Dramatica se pueden encontrar abundantes enlaces a casos de tecnoembaucamiento histórico. Al explorar estos linajes podemos entender mejor qué es lo que convierte a Anonymous —tanto los trols como los activistas— en algo diferente dentro de un panteón más amplio de embaucadores tecnológicos.

(Breve) Historia natural del embaucamiento en Internet (o Genealogía de la falta de moral)

Weev es un trol de trols, un espécimen raro en un campo que genera principalmente muchas variedades de plantas.

La ascendencia de los trols presume de un elenco de personajes bastante variado y ecléctico. El troleo era una actividad común en el universo underground de los hackers, un lugar para los hackers subversivos que prosperaron en las décadas de 1980 y 1990, buscando conocimientos prohibidos hurgando, sin que nadie los invitara, en los ordenadores de otras personas. Pero incluso ellos deben agradecer a sus antepasados directos, los phreaks, la estética de la audacia. Mediante la fusión de la espeleología tecnológica y la gamberrada, los phreaks entraban ilegalmente en el sistema telefónico recreando las frecuencias de audio utilizadas por el sistema para dirigir las llamadas. Esos tíos lo hacían, sin lugar a dudas, para aprender y explorar. Pero la emoción de la transgresión era igualmente esencial para el placer del phreaking. En las décadas de 1960 y 1970, los phreaks***** empleaban sus habilidades para reunirse en *party lines* de conferencias telefónicas. El phreaking atrajo a algunos chicos ciegos, que hallaron una fuente de libertad al poder conectarse telefónicamente con otras personas. A través de los cables telefónicos de todas partes, las personas que no podían verse entre ellas se reunían para conversar, chismorrear, compartir datos tecnológicos y planear y ejecutar travesuras. Muchas travesuras. Naturalmente, la mayoría de ellas implicaban llamadas telefónicas. Aunque la mayoría eran alegres y ligeras, algunas exhibían un lado inquietante. Phil Lapsley, un historiador de los phreaks, relata una famosa broma gastada en 1974 en la que los phreaks aprovecharon un extraño error producido en el sistema telefónico para redirigir todas las llamadas efectuadas a residentes en Santa Bárbara, California, a un trabajador de un servicio de emergencias falso que les advertía: «Se ha producido una explosión nuclear en Santa Bárbara y todas las líneas telefónicas están fuera de servicio.»[18] Weev, que no ignora la historia, adora las bromas telefónicas y se

considera un heredero de este ilustre linaje.

El final de la red telefónica analógica, después de la desinversión de “Ma Bell” (el nombre cariñoso dado a AT&T por los phreaks), significó el fin de la edad dorada del phreaking. Fue reemplazado en gran medida por la exploración de las redes informáticas, dando origen al underground hacker, que alcanzó su máxima expresión en la década de 1990. Si bien muchos de estos hackers adquirieron, hicieron circular y produjeron conocimientos técnicos —buscando vulnerabilidades de seguridad y creando curiosidades técnicas— también eran expertos en la fruta prohibida. Por lo tanto, no debe extrañar que sus acciones se extendieran desde las participaciones estrictamente técnicas hacia aquellas que incluían burlas, espectáculo y transgresión. Estos hackers establecieron rápidamente una clara diferencia entre su política y su ética con respecto a la que practicaban sus homólogos universitarios del Instituto Tecnológico de Massachusetts (MIT), Carnegie Mellon y Stanford. Estos hackers, que en la década de 1960 permanecían despiertos toda la noche para poder acceder a sus amados ordenadores, que durante el día solo podían utilizarse para cuestiones oficiales, han sido descritos majestuosamente por el periodista Steven Levy.[19] Aunque estos primeros hackers también mostraban cierta afinidad con las gamberradas, se atenían a un *ethos* de acceso y transparencia más sólido que los hackers underground.

Muchos hackers underground se mostraban juguetones en sus actividades de hackeo y bromas de gusto diverso. Eran revoltosos y vagabundos felices. Había, no obstante, una cohorte de hackers underground que guardaba una gran semejanza con el arquetipo de Loki en sus excursiones y cacerías en la red. Cuando entrevisté a los hackers que habían estado activos en la década de 1990 acerca de sus actividades de troleo, la conversación se dirigió inevitablemente hacia un debate sobre el hacker/trol más temido de la época: “uƐea” (pronunciado “euforia” y extrañamente similar a “lulz” en su figuración). El reino de este trol era tan aterrador que cada vez que pronuncio u4ea ante uno de sus contemporáneos, su comportamiento se altera y los procedimientos asumen una seriedad incomparable. U4ea es canadiense. Y lo que es más notable, este trol fue «fundador, presidente y dictador vitalicio» del grupo de hackers BRoTHeRHooD oF WaReZ —(“Bo W” en su forma abreviada; Warez significa software pirateado — “Bo W” buscaba burlarse de los grupos de copias piratas del Sistema de Tablón de Anuncios). Según un ex miembro con quien mantuve varios chats online, el “ala paramilitar” de BoW, llamada Hagis (abreviatura de Hackers against Geeks in Snowsuits, o “Hackers contra Geeks en Trajes de Nieve”), continuó lanzando campañas crueles de hackeo y bromas humillantes contra

víctimas que incluían desde corporaciones, hackers "de sombrero blanco" –respetuosos de la ley– y gurús de la seguridad informática, hasta básicamente cualquiera que se encontrase en su línea de fuego. A modo de ejemplo, a finales de la década de 1990 a Hagis se le fue la pinza durante una disputa multianual con un hacker de sombrero blanco llamado Jay Dyson. En primer lugar fueron a por su proveedor de servicios de Internet, borrando *todos* sus archivos y dejándolos desconectados durante dos semanas. Luego procedieron a borrar archivos en el sitio web empresarial de Dyson. No satisfechos con estas acciones, acosaron a su esposa con mensajes amenazadores, informándole a través de su correo electrónico hackeado de que «Toda la familia Dyson pagará por los errores de Big Jay».[20]

Después de tener conocimiento de éste y otros ataques por el ex miembro de BoW con el que chateaba, escribí:

<biella>: despiadado, tío
<hacker>: sí, éramos un grupo bastante jodido al punto de que desaparecí del mapa
<biella>: ¿por qué? quiero decir, ¿qué era lo que impulsaba a esos tíos? ¿es solo porque podían hacerlo?
<hacker>: no tengo la más remota idea si te soy sincero
<hacker>: había un montón de guerras de hackers de las que nadie sabía nada
<hacker>: los servidores irc desaparecían, los ISP quedaban borrados de la faz de la tierra durante días o semanas
<hacker>: pero todo quedaba en casa
<hacker>: los medios solo captaban pequeñas pistas
<hacker>: quiero decir, era una época en la que los hackers no querían llamar la atención, la gente que hablaba con la prensa eran tíos que habrían hecho cualquier cosa por aparecer en la tele
<hacker>: éramos una verdadera subcultura, nuestras propias noticias, nuestros propios famosos, nuestra propia jerga, nuestra propia cultura

Y no pude evitar añadir:

<biella>: y vuestras propias guerras

Aun así, Hagis también podía ser bastante bromista. En una ocasión desfiguraron el sitio web de Greenpeace y colgaron lo que hoy se podría considerar un mensaje clásicamente lulz concebido para divulgar el calvario de un phreak y hacker llamado Kevin Mitnick al que habían arrestado: «Liberad a Kevin Mitnick o mataremos a palos a 600 crías de foca.»[21]

Después de haber alcanzado esta profundidad (es decir, rascar apenas la

superficie), decidí que mis interlocutores tenían razón: era hora de que levantase el pie del acelerador en mi búsqueda de uɛea. Apenas se había escrito nada sobre este famoso trol…, y por una buena razón.

El troleo en la década de 1990 también seguía un vector diferente hacia el anonimato. Al margen de estas guerras ocultas y elitistas de los hackers, los usuarios corrientes tuvieron su primera experiencia amarga de troleo en Usenet, el influyente tablón de megamensajes. En 1979, Internet existía como una red militar y académica —la ARPANET— y el acceso estaba limitado a una selecta minoría. Naturalmente, unos cuantos ingenieros crearon un nuevo sistema, Usenet, al que concibieron como «la ARPANET de los pobres». Concebido al principio con el único propósito de examinar oscuras cuestiones técnicas, el sistema no tardó en multiplicarse —para sorpresa de todo el mundo— para incluir centenares de listas con debates animados y, en ocasiones, feroces. El contenido técnico fue ampliado por grupos dedicados al sexo, el humor, las recetas y (naturalmente) la antiCienciología.

Usenet y otras listas de correo electrónico fueron también los lugares donde el término “trol” se incorporó inicialmente al uso común. Hacía referencia a las personas que no contribuían de modo positivo a los debates, que discutían por discutir o que simplemente eran molestos gilipollas (deliberadamente o no). Los usuarios de las listas advertían a menudo a los otros que «dejasen de alimentar a los trols», un refrán que aún se puede ver habitualmente en las listas de correo electrónico, tablones de mensajes y las secciones de comentarios en los sitios web.

Pero Usenet también reprodujo y alimentó la espectacular especie de trol que saboteaba deliberadamente las conversaciones, provocando la exasperación de los miembros de la lista y, sobre todo, de los administradores de la misma. En este sentido, no existe mejor ejemplo que el de Netochka Nezvanova, nombre del personaje principal en la primera (y fallida) incursión de Dostoievski en el terreno de la novela. El nombre, propiamente, significa “nadie sin nombre”. Y, del mismo modo que ocurre con Anonymous en la actualidad, se cree que muchos grupos e individuos han adoptado ese apodo, convirtiéndolo en un ejemplo adecuado de lo que Marco Deseriis, el experto en medios de comunicación, describe como un «nombre de uso múltiple», en el que «el mismo alias» es adoptado por «colectivos organizados, grupos afines y autores individuales».[22]

La declaración artística de Netochka Nezvanova, publicada en la red, recoge el estilo demencial y fogoso que impulsa a este personaje:

> InterCuerpo—Declaración Artística
>
> Internet—donde uno puede acceder a la propuesta + los materiales pertinentes
>
> Nuestros cuerpos son las fronteras de nuestra comprensión.
>
> Los universos son el cuerpo. Internet es la piel.
>
> Éste es mi Inter Cuerpo. Soy Soft Wear.
>
> Cuando estoy sola quiero que entres dentro de mí, deseo usarte.
>
> Disueltos e integrados, somos desglosados en una topología nómada e inestable de cintas cerámicas y canales microfluidos, de innumerables destellos fosforescentes de las trasposiciones inexpugnables de los signos visibles de los encuentros misteriosos e invisibles en sueños divisibles.

Después de haber leído este texto, tal vez te encuentres, como me sucedió a mí, excavando en tus sensibilidades imaginativas, deleuzianas, a menos que estuvieras en alguno de los mailings de correo electrónico que ella destrozó. Su personaje se inmiscuía con tanta frecuencia, con tanta habilidad y en tantos grupos nuevos y listas heterogéneas, que los distintos administradores de listas se unieron en una lista especializada propia, con el exclusivo propósito de hacer frente al rastro de destrucción que dejaba a su paso. En mi universidad actual, McGill, Netochka Nezvanova participó en una lista de correo electrónico sobre Max, un lenguaje de Programacion visual para música, audio y medios de comunicación, pero fue expulsada en 2001 después de que amenazara con demandar a miembros particulares de la lista. Éste es un fragmento de los motivos expuestos para prohibir su participación:

> Segundo, después de que “ella” fuese excluida del mailing de McGill, inició lo que podría describirse como una campaña de terror que incluía enviar correo basura a todos aquellos que estuvieran en la lista de Max, ataques de denegación de servicio, y correos electrónicos amenazadores y calumniosos enviados aleatoriamente a personas de McGill. No tenía ningún sentido que mis compañeros de trabajo y yo nos sometiésemos a esta clase de hostigamiento. Sin embargo, resulta que muchos de estos actos son delito. Si este comportamiento se repite, las víctimas del mismo pueden interponer acciones legales y yo sugeriría enfáticamente que así lo hagan.

A modo de reacción, alguien que figuraba en la lista se quejó: «Ya estamos, ¡otra vez la censura!».[23]

En la década de 1990 Usenet y muchos otros mailings de correo electrónico florecientes promovieron una libertad de expresión incontrolada y fueron aplaudidos por ello. Pero los trols como Netochka forzaron un debate, que aún hoy nos acompaña, acerca de los límites que debe tener ese discurso: ¿deberían las listas de correo electrónico y los moderadores de las páginas web reprimir el lenguaje ofensivo en nombre del civismo, algo considerado necesario por algunos para una comunidad sana? ¿O deberían evitar la censura del discurso, no importa cuán cuestionable sea, para que Internet pueda ser un lugar donde la libertad de expresión se manifieste de manera incondicional?

Cabe señalar en particular —mientras rastreamos nuestro linaje de troleo a través del tiempo— la evolución registrada por 4chan, un tablón de imágenes modelado sobre el popular tablón de imágenes japonés Futaba Channel, conocido también como 2chan ("chan" es la abreviatura de "channel"). Es aquí, tal vez más que en cualquier otro lugar, donde hizo su aparición el tipo populista de troleo que se conoce hoy. 4chan es único por su cultura de permisibilidad extrema —haciendo que las cuestiones relativas a la libertad de expresión sean absolutamente irrelevantes— impulsado por una cultura de anonimato adoptada por sus usuarios. Naturalmente, fue en este tablón donde nacieron la idea e identidad colectivas de Anonymous. A diferencia de Usenet, nadie en 4chan está preocupado en absoluto por el discurso incivil que se propaga a través del tablón cada segundo del día. En muchos aspectos, el tablón está concebido explícitamente como una zona donde «se puede-decir-cualquier-cosa»: cuanto más ofensiva y grosera, ¡coño!, mejor.

Desde su lanzamiento en 2003, 4chan se ha convertido en un tablón de imágenes inmensamente popular, icónico y abusivo. Compuesto por más de sesenta foros temáticos (en el momento de escribir este texto) que van desde el *anime* hasta la salud y la forma física, es a la vez fuente de muchos de los artefactos culturales más venerados de Internet (como los memes Lolcats, la combinación de la fotografía de un gato con un texto humorístico) y una de sus colmenas de basura y canalladas más horribles. El foro "Random", llamado también "/b/," rebosa de pornografía, agravios raciales y un estilo de humor característico derivado de la humillación. Es el lugar donde una vez floreció el troleo. Un "/b/tard" (como se denomina a quienes frecuentan este foro) le explicó a mi clase que «todo el mundo debería tener la percepción de que /b/ es un desmadre casi completamente sin filtrar de cualquier cosa que os podáis imaginar y de un montón de cosas que no podríais o no querríais imaginar». Una entrada

podría incluir a una mujer desnuda acompañada de la petición: «puntúa a mi esposa». La entrada siguiente podría mostrar una imagen particularmente repugnante de un cuerpo severamente mutilado, pero quizás seguida luego de una muestra de humor ligero:

Archivo : 1291872411.jpg-(10 KB 292x219, bicarbonato de sodio.jpg)

☐ **Anonymous** 12/09/10(Jue)00:26:51 No.293326XXX ¿Qué puede pasar si tomamos solo media cucharadita de bicarbonato de sodio?



☐ **Anonymous** 12/09/10(Jue)00:28:24 No.293326XXX bump

☐ **Anonymous** 12/09/10(Jue)00:29:12 No.283326XXX >>293326451 eso no es mucho. Sugiero agua. Luego eructar.

☐ **Anonymous** 12/09/10(Jue)00:33:06 No.293327XXX FFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFF COMER MÁS Y DESPUÉS BEBER COLORANTE ROJO PARA ALIMENTOS Y VINAGRE Y ESPERAR LA REACCIÓN Y CORRER A LA HABITACIÓN MÁS CERCANA LLENA DE GENTE Y GRITAR, "¡SOY EL DIOS DE LOS VOLCANES, TOAN GLADIUS! BLBLBLBLBLBLBLBLBLBLBLBL!"

En general, sin embargo, gran parte del material está diseñado para escandalizar a los no iniciados, una valla fronteriza construida discursivamente y destinada a mantener a los no iniciados —apodados "n00bs" o "newfags"— lejos, muy lejos. (Prácticamente todas las categorías de persona, desde los más veteranos hasta los recién llegados, son catalogadas como "maricón". En 4chan es a la vez un insulto y una expresión de cariño. En este libro veremos el sufijo -*fag* muchas veces.) Para los iniciados, es el estado de cosas normal y una de las características definitorias y atractivas de este tablón.

En 4chan se desanima claramente a los participantes a identificarse y la mayoría incluye sus entradas bajo el nombre predeterminado de "Anonymous", como se observa en el ejemplo mostrado más arriba. Técnicamente, 4chan

mantiene registros de direcciones IP y no hace nada para impedir que los visitantes sean identificados. A menos que los usuarios oculten sus direcciones antes de conectarse, el fundador, propietario y administrador de sistemas del sitio — Chris Poole, alias "moot"— tiene total acceso a ellas. Poole incluso se las ha entregado a la policía para colaborar con investigaciones legítimas. (Esta política es ampliamente conocida entre los usuarios.) Pero, al menos en un sentido práctico (y al menos entre sus usuarios como compañeros), el tablón funciona de manera anónima; excepto en raras excepciones, y en el caso ocasional donde el sujeto de una discusión debe identificarse utilizando una fotografía con una fecha, los usuarios se relacionan sin ningún apodo o nombre de usuario. Las entradas son eliminadas rápidamente de la página principal —para ser borradas del servidor cuando llegan a la página 14— sobreviviendo solo en la medida en que los usuarios sigan mostrando interés en ese tema. Eso «reduce la responsabilidad personal y estimula la experimentación», según el experto en medios de comunicación Lee Knuttila.[24] La experimentación incluye generar memes (se trata de modificaciones de imágenes, vídeos o eslóganes humorísticos, algunos de los cuales alcanzan un estatus legendario), feroces campañas de troleo orquestadas por Anonymous (aunque esta actividad ha sido menos común en los últimos años) e incesantes burlas y acusaciones denigrantes de otros usuario (tales como incitar a personas con ideas suicidas a «simplemente hazlo» y «conviértete en un héroe»). Cabe señalar, sin embargo, que existen también abundantes consejos compasivos y sensibles, especialmente para aquellos que buscan ayuda en sus relaciones o cuando alguien descubre el vídeo de un gato al que están torturando. Pero este aspecto raramente aparecía en las noticias.

Todo esto sucede con el conocimiento de la impermanencia. A diferencia de lo que ocurre con los mailings de correo electrónico u otras clases de tablones virtuales, no existe ningún archivo oficial. Si un hilo de ejecución no "rebota" nuevamente hacia arriba en el tiempo de respuesta, muere y se evapora. En un canal activo, como es el caso de /b/, todo este ciclo vital se produce en pocos minutos.

En este entorno resulta difícil que una persona pueda acumular estatus o reputación, y muchos menos fama. Contra este fondo de experimentación cacofónica y de acciones efímeras se han formado no obstante una memoria e identidad colectivas sólidas alrededor de campañas de troleo legendarias, toda clase de bromas para iniciados y artefactos tales como macros de imágenes. En términos estéticos, cuanto más extremo sea un contenido, mejor será, ya que de este modo se asegura el interés de los participantes, y se estimulan las respuestas a los hilos de ejecución (manteniéndolos activos). En casos particularmente

novedosos, un contenido extremo puede llegar a circular incluso más allá del tablón, hasta alcanzar tierras lejanas como la comunidad de tablones de mensajes, reddit, o bodybuilding.com, y, finalmente, despertar una masiva conciencia cultural. No olvidemos que los lolcats tuvieron su pistoletazo de salida en 4chan. Los trols, en particular, centran su atención en la búsqueda colectiva de victorias épicas, que es solo una forma de contenido entre muchas otras. (Para que quede claro, 4chan alberga a muchos trols, pero muchos participantes se mantienen al margen de las actividades propias del troleo. Otros incluso evitan completamente esa actividad y permanecen allí como simples espectadores o acechadores.)

Resulta prácticamente imposible determinar el día o el acontecimiento que inició el troleo en 4chan. Pero en 2006, el nombre Anonymous era utilizado por los participantes para intervenir en incursiones de esta naturaleza. Estas invasiones continuarían durante muchos años, incluso después de que se desplegase de forma rutinaria con fines activistas. Por ejemplo, en 2010 Anonymous intentó "arruinar" a una preadolescente llamada Jessi Slaughter después de que colgase en 4chan sus monólogos caseros, que habían adquirido cierta notoriedad en el sitio de cotilleos StickyDrama. Anonymous decidió actuar debido a los alardes descarados de Slaughter —en uno de los vídeos afirmaba que «dispararía una glock en tu boca y te haría papilla el cerebro»— y publicó su número de teléfono, dirección y nombre de usuario de Twitter, inundándola con correos electrónicos llenos de odio y falsas llamadas amenazadoras, haciendo circular imágenes de ella tratadas con Photoshop y remezclas satíricas de sus vídeos. Cuando su padre grabó una airada protesta, en la que afirmaba que había "descubierto" a quienes atormentaban a su hija y los había denunciado a la "ciberpolicía", también se convirtió en objeto de burla. Slaughter, descrita por los participantes de /b/ como una "lulzcow ... puta", está incluida hoy en el Urban Dictionary como «la personificación de once años de una zorra/*poser*/desecho de internet/aspirante a la *scenecore*».

Por una parte, las incursiones de troleo extravagantes y las declaraciones denigrantes como "lulzcow ... puta" (o el «debido a un fallo y al SIDA» de las incursiones en el hotel de Habbo) funcionan para los usuarios de 4chan como un repelente destinado a mantener a los usuarios ingenuos alejados de su terreno de juego en Internet. Por otra parte, cuando se lo compara con la mayoría de los otros escenarios donde actúan los trols —como la GNAA de weev— 4chan es una Meca del troleo populista. Por populista me refiero simplemente a que la pertenencia a 4chan está a disposición de cualquiera que desee cruzar estos límites, disponga de tiempo para aprender la jerga y (por supuesto) tenga estómago para soportar la carnaza. El protocolo y las técnicas que emplean los

usuarios de ɛchan son solo superficialmente elitistas. Un ex estudiante de mis clases me proporcionó la siguiente visión. El tío, excepcionalmente inteligente, también era un trol, o un *goon* para ser más precisos, ya que es así como se denominan ellos mismos en Something Awful (Algo espantoso), su sitio web elegido en aquella época:

> Something Awful es como el exclusivo club de campo de Internet, con una cuota única de 10 pavos, una larga lista de reglas muy particulares para SA, moderadores que pueden prohibir y legalizar, y la ejecución comunitaria de "Buenos Posts" a través del ridículo. 4chan, por otra parte, es una ley de la selva orgánica que no obliga tanto como hace participar a su grupo amorfo de socios en una batalla a megamuerte por el primer puesto en el humor. Cualquiera puede participar en 4chan y la fama de Internet no es posible de la misma manera que lo es en SA porque todo el mundo es literalmente anónimo.

Cualquier contenido que se despliegue en el tablón —ya se trate de una broma, una larga conversación o una campaña de troleo de tres días de duración—, para 4chan el anonimato es esencial; se podría decir que el anonimato es tanto su regla básica como su rasgo cultural dominante, un principio fundamental heredado por Anonymous, incluso en su seudónimo, como la extensión material en forma de multitudes de portadores de la máscara de Guy Fawkes. En 4chan se produce una interacción entre la *función* del anonimato (que permite la competición pura sin la interferencia de la reputación o el capital social) y los *efectos* del anonimato (los memes, hackeos y actos de troleo que se producen y tienen un impacto concreto en el mundo). A diferencia de los egoístas actos de troleo de weev, la acción colectiva de la "Máquina de Odio del Internet" de Anonymous en 4chan absuelve a los individuos de toda responsabilidad en el sentido convencional, pero no en un sentido colectivo.[25] Es decir, Anonymous está abierto a cualquiera que desee sumergirse en un colectivo capaz de obtener la fama mediante acciones como las incursiones en el Hotel Habbo. Carente de cualquier reconocimiento individual, cada actividad se atribuye a un seudónimo colectivo, una reencarnación de Netochka Nezvanova. En 4chan, los participantes también avergonzarán a todos aquellos que buscan celebridad y atención usando su propio nombre, y les dedicarán namefags.

Como equipo de troleo, Anonymous consiguió una considerable notoriedad en los medios de comunicación, igual que ha sucedido con weev. En ciertos aspectos, el colectivo se hizo famoso. Sin embargo, mientras que, por una parte, las proezas del troleo de Anonymous y los usuarios de 4chan, y por otra, las de

weev, están conectadas por sus enfoques tácticos, también representan estratos entre ellos. Independientemente de la extensión que alcance la fama de Anonymous, la identidad personal y el individuo siguen subordinados a un foco de atención en la victoria épica y, especialmente, en el lulz.[26]

Esta inclusión de la identidad individual en la identidad colectiva es algo inusual en la cultura occidental, y entender su asimilación es crucial para nuestro conocimiento de la formación de Anonymous como grupo activista. Es muy posible que la naturaleza desagradable de las primeras actividades de troleo llevadas a cabo por Anonymous motivase el colectivismo como un elemento de seguridad; probablemente los participantes tenían el deseo de participar, de recibir un pago en lulz, sin correr el riesgo de ser identificados y estigmatizados por la sociedad. Para entender estas motivaciones, y la poderosa relevancia de la voluntad de un individuo de subsumir su identidad, examinaremos brevemente la cultura de la búsqueda de fama —de la celebridad individualista— en sí misma.

El truco del embaucador de Anonymous: desafiar la celebridad individual mediante la celebridad colectiva

Actualmente, la búsqueda de la fama impregna prácticamente todas la esferas de la vida estadounidense, desde los medios de comunicación, que contratan a celebridades de Hollywood como presentadores de las noticias, hasta las plataformas de micromedios que proporcionan infinitas oportunidades para el narcisismo y el autoengreimiento; desde los salones del mundo académico, donde profesores superestrellas perciben elevadas nóminas, hasta los escenarios deportivos, donde los jugadores se embolsan salarios realmente obscenos. El comportamiento que busca la fama refuerza lo que el antropólogo David Graeber, basándose en el influyente trabajo de C. B. Macpherson, identifica como «individualismo posesivo», definido como «esos hábitos de pensar y sentir profundamente interiorizados» mediante los cuales vemos «todo lo que nos rodea fundamentalmente como una propiedad comercial real o potencial».[27]

¿Cómo consiguió ɛchan —uno de los sitios más sórdidos de Internet— incubar uno de los ejemplos más sólidos de ética colectivista y antifama sin que sus miembros ni siquiera se lo hubieran propuesto? Está ética prosperó orgánicamente en 4chan porque podía ser ejecutada de una forma no adulterada. Durante una charla para mi clase, un activista actual y ex trol de Anonymous explicó el papel fundamental desempeñado por 4chan en la consolidación de lo que él llama “el ideal primordial de Anonymous”:

> Los posts en 4chan no tienen nombres y tampoco marcadores identificables asociados a ellos. El único elemento por el que puedes juzgar un post es por el contenido y nada más. *Esta eliminación de la persona, y por extensión todo lo que se asocia a ella, ese liderazgo, representación y estatus, es el ideal primordial de Anonymous.* [cursiva de la autora]

Este Anon, que disertaba de forma anónima a través de Skype para mis diez embelesados alumnos, ofreció inmediatamente una serie de astutas cualificaciones respecto de este ideal primordial: la autoexclusión del individuo. Cuando Anonymous abandonó 4chan en 2008 en busca de objetivos activistas, según explicó, este ideal fracasó, a menudo de manera espectacular. Una vez que los individuos se relacionaban a través de seudónimos o se conocían personalmente, las conductas de búsqueda de estatus les servían para reafirmarse. Los individuos maniobraban y presionaban en pos del poder.

Sin embargo, el tabú de la búsqueda de fama estaba tan arraigado en 4chan, y era tan valorado por su éxito, que impedía en gran medida, salvo unas pocas excepciones, que estas luchas internas por el estatus se extendieran a búsquedas públicas de fama personal. (Más tarde veremos su mayor fracaso en los microsistemas de grupos de hackers como AntiSec y LulzSec, análogos a las estrellas de rock en su capacidad de acumular fama y reconocimiento y —no es de extrañar— de desatar la ira de algunos Anons, incluso mientras eran admirados por sus bufonadas políticas en el reino del lulz.)

Una vez que Anonymous abandonó 4chan para participar en el activismo, el ideal contra la búsqueda de la celebridad se convirtió en algo «más matizado... encarnado en el deseo de ausencia de liderazgo y alta democracia», según las palabras de este Anon. Los intentos de llevar estos principios a la práctica también se tradujeron en errores, sobre todo en la aparición de pequeños grupos que concentraban el poder.

Pero a pesar de la fragmentación en grupos y élites, los ideales generales continuaron vigentes. La adhesión significaba «que cualquiera [podía] llamarse a sí mismo Anonymous y reclamar el nombre de forma legítima», como explicó el disertante. Esta libertad para adoptar el nombre y experimentar con él es precisamente lo que permitió que Anonymous se convirtiese en la astuta Hidra que es en la actualidad.

Pero si miramos detrás del ideal —la noción de que Anonymous es propiedad de todo el mundo, una identidad común, por así decirlo—, nos encontramos ante una realidad mucho más compleja. Y fue aquí, en este punto matizado, donde este Anon acabó su microdisertación. Creo que mis estudiantes

estaban hipnotizados y a la vez conmocionados de que alguien de Anonymous pudiera ser tan inteligente y elocuente; les expliqué que se puede entender a Anonymous como lo que el antropólogo Chris Kelty ha llamado jocosamente, en oposición al subalterno, el “superalterno”: esos *geeks* con una excelente formación que no solo hablan por sí mismos sino que responden de manera enérgica y crítica a aquellos que pretenden hablar por ellos.[28] El ponente invitado de Anonymous continuó:

> A la mayoría de nosotros nos impulsa el humor. De modo que no debiera extrañar a nadie que a menudo compitamos para hacerles un favor con otros grupos que adoptan el nombre de Anonymous, tales como... los nuevos Anons exclusivamente activistas de Occupy Wall Street, o los teóricos de las conspiraciones y otros colectivos serios que reivindican el nombre. Es verdad. No podemos negarles el nombre. Pero lo que es importante eliminar de esta conversación es que en ninguna parte del ideal de Anonymous se estipuló jamás que Anonymous deba permanecer unido a otros Anonymous o que ni siquiera le gusten. De hecho, la animosidad y las guerras entre gupos que reivindican el nombre de Anonymous están en consonancia con los proyectos originales basados en Internet que llevan a cabo los Anons culturales.

Es en este punto donde podríamos entender la complejidad de Anonymous. Hay una idea y un tema singulares animando su espíritu y los participantes intentan presentarlo como un frente unido. Para los medios de comunicación resulta tentador comprar en este mercado al por mayor de marcas, presentar a Anonymous como sus valores y su envoltorio. Pero la realidad de la composición del grupo, en todos sus variados tonos y matices, es imposible de presentar en un solo boceto, aun cuando Anonymous utilice un único nombre. Su afiliación incluye a demasiadas redes y grupos de trabajo distintos, cada uno de los cuales mantiene diferencias con el otro en distintos momentos. La propia naturaleza de este colectivo de colectivos significa que la acumulación de demasiado poder y prestigio —especialmente en un único punto en el espacio (virtual)— no solo es tabú sino también funcionalmente complicado.

4chan era una zona cero para una consistente ética antifama, un sistema de valores opuesto al auto engrandecimiento y al aparato de los medios de comunicación dominantes (uno de los cánceres que destruye a /b/, como le gusta decir a Anonymous). Esta concepción de la ética se transmitió a la encarnación activista de Anonymous. Es en estas prácticas alternativas de la sociabilidad —que alteran la división ideológica entre individualismo y colectivismo— donde

podemos reconocer la evolución del troleo hasta convertirse en un arma cargada de principios contra los bancos monolíticos y las oscuras empresas de seguridad. La colectividad está ampliando su cuota de mercado: desde el movimiento de globalización controlado opuesto a las corporaciones de hace una década, hasta Anonymous y el reciente estallido de movimientos que carecen de liderazgo como Occupy Wall Street. A menudo esta realidad queda totalmente perdida en los medios de comunicación dominantes, que no pueden —o no quieren— redactar una historia que no normalice la conversión de un individuo en líder o famoso, completado con alguna muestra de heroísmo individual o de trágicas flaquezas morales. Esto, por supuesto, no es solo una tendencia del periodismo y los periodistas. La mayor parte de la filosofía occidental y, a su vez, más generalmente gran parte de la cultura occidental, ha puesto el yo —el individuo— como el lugar de la investigación epistémica. Es difícil sacudirse milenios de pensamiento filosófico sobre un tema, alejar un pensamiento intelectual que también es sentido común cultural.

Es por esta razón que Anonymous, ya sea en sus actividades de troleo o en sus encarnaciones activistas, actuaba como una fuerza de engaño parecida al jujitsu, siendo sus maquinaciones incomparables con la lógica impulsora de los medios de comunicación corporativos dominantes y las sensibilidades hegemónicas del yo. Volvía un poco locos a los periodistas, algo que pude presenciar de primera mano cuando hice de intermediaria, un poco a la manera de los embaucadores, entre Anonymous y los medios de comunicación. A menudo ayudaba a la prensa a cruzar ese profundo abismo a paso de caracol cuando trataban de identificar a un líder, o al menos a algún personaje, que pudiera satisfacer las demandas explícitas de su profesión.

Tal vez se deba a esta misma resistencia de la convención periodística —al deseo de descubrir, revelar o directamente crear un líder famoso— que los periodistas se veían obligados a cubrir el tema de Anonymous. La búsqueda de un portavoz, un líder, un representante fue en vano, al menos hasta que el Estado decidió intervenir y comenzó a arrestar a los hackers. Pero, en su mayoría, a los medios de comunicación se les ofrecía apenas un puñado de personajes alrededor de los cuales era fácil poder construir una historia.

Lo que comenzó como una red de trols se ha convertido, en su mayor parte, en una fuerza positiva en el mundo. La aparición de Anonymous desde uno de los lugares más sórdidos de Internet es una historia de prodigios, de esperanza y de ilusiones lúdicas. ¿Es posible realmente que estos ideales de colectivismo e identificación grupal, forjados como lo han sido en las fraguas infernales, aterradoras, del troleo, pudieran trascender semejante estado original? ¿Cristalizó

realmente el sumidero de 4chan en uno de los grupos activistas políticamente más activos, moralmente fascinantes y subversivamente prominentes que operan en la actualidad? Aunque resulte sorprendente, sí. Veamos cómo ocurrió.

Capítulo 2

Proyecto Chanology:
vine por el lulz pero me quedé por la indignación

Fueron numerosas las contingencias que convergieron para despertar a los embaucadores-trols del desagradable submundo del 4chan. Pero si tenemos que aislar un único hecho como el mayor responsable de que esto sucediera, sería la filtración en Internet del vídeo de la Iglesia de la Cienciología en el que aparece Tom Cruise, el más famoso de los famosos de la Cienciología. «Streisand estaba en todo su esplendor», bromeó un Anon. El llamado "Efecto Streisand" es un conocido fenómeno de Internet mediante el cual el intento de censurar una información consigue el efecto contrario: más personas quieren conocerla para entender el motivo de la censura y, por lo tanto, se extiende aún más que si la hubiesen dejado en paz. El fenómeno lleva ese nombre después del intento de Barbra Streisand en 2004 de prohibir, a través de una demanda multimillonaria, que se publicaran unas fotografías aéreas de su mansión en Malibú. El fotógrafo solo estaba tratando de documentar la erosión producida en esa zona de la costa de California. Antes de la presentación de la demanda, la imagen de la casa de la estrella solo había sido vista seis veces por la red, pero después de que el caso se hiciera público, el sitio tuvo más de 420.000 visitas. El vídeo de la Cienciología grabado por Tom Cruise se vio sometido a una dinámica similar; su circulación se volvió imparable.

En el vídeo, Tom Cruise personifica la visión narcisista del mundo que tiene la Cienciología: «Ser un cienciólogo es... cuando pasas junto al lugar de un accidente, no es como si lo hiciera cualquier otra persona», dice Cruise con una sonrisa de autosatisfacción. «Cuando pasas por allí sabes que tienes que hacer algo porque eres el único que realmente puede ayudar.» Los *geeks* de

Internet (junto con casi todos los demás) consideraron el vídeo como un intento patético (por no decir hilarante) de conceder credibilidad a aquella pseudociencia a través de la intervención de un famoso. Mientras en el vídeo Tom Cruise se reía encantado de sí mismo, la comunidad de Internet se reía a carcajadas —aunque por razones muy diferentes— de él.

El vídeo llegó inicialmente a Internet no gracias a los esfuerzos de Anonymous, sino a través (de manera muy conveniente) de una filtración anónima. El vídeo debía aparecer originariamente en la NBC para que coincidiera con el lanzamiento de la biografía no autorizada de Tom Cruise, pero en el último momento la cadena se echó atrás. Sin embargo, los críticos de la Cienciología se movieron rápidamente para asegurarse de que el vídeo encontraba su camino en la red. La excienciólogа Patty Moher, en colaboración con la veterana crítica Patricia Greenway, envió una copia a Mark Bunker, quien subió el vídeo y envió un enlace al periodista de investigación Mark Ebner, quien a su vez lo envió a otras fuentes de noticias. Gawker, Radar y otros sitios lo recogieron el 13 de enero de 2008, asociándolo a otro vídeo subido por Bunker con protección de contraseña —o, al menos, eso pensó. Estaba equivocado. «Me desperté unas horas más tarde para descubrir que el capítulo que contenía el monólogo de Cruise no se había colocado, accidentalmente, en ‘privado’ —manifestó posteriormente—. Había sido visto cerca de 20.000 veces mientras yo dormía y fue descargado y copiado en múltiples ocasiones en numerosas cuentas por personas que habían leído las noticias en Gawker y Radar y otras coberturas del vídeo.»[29] YouTube procedió posteriormente a eliminar los vídeos de Bunker alojados en el canal “TomCruiseBook”, junto con todo el canal, probablemente a instancias de la notificación de un aviso de derechos de autor de la Cienciología.

El 15 de enero, Gawker volvió a publicar el vídeo acompañado de una descripción breve e impactante adaptada para millones de globos oculares: «Permitidme que lo explique de esta manera: si Tom Cruise saltando sobre el sofá de Oprah registró un 8 en la escala de “aterrador”, esto es un 10.» El Centro de Tecnología Religiosa —la rama de la Cienciología que aborda las cuestiones relacionadas con la propiedad intelectual— pasó inmediatamente a la acción, amenazando con demandar a los editores si no eliminaban el vídeo. Gawker terminaba su artículo con una muestra de valentía: «Es de interés periodístico y no lo eliminaremos.»[30] El secreto había sido revelado, los tíos de la Cienciología estaban furiosos (y a punto de repartir furiosas demandas) y entonces todo estalló cuando la “colmena”, como se llamaba a menudo a

Anonymous en aquella época, decidió entrar en escena.

El 15 de enero, a las 19:37:37 h, las puertas del submundo se abrieron con un hilo histórico sobre el activismo dirigido hacia la Cienciología:

Archivo :1200443857152.jpg-(22 KB, 251x328, intro_scn.jpg)

☐ **Anonymous** 01/15/08(Jue)19:37: 37 No.51051816



Creo que ha llegado el momento de que /b/ haga algo grande.

La gente necesita entender que no debe joder con /b/, y no hablar de nada durante diez minutos, y esperar a que la gente entregue su dinero a una organización que no tiene absolutamente ningún puto sentido.

Estoy hablando de "hackear" o "eliminar" el sitio web oficial de la Cienciología.

Es hora de utilizar nuestros recursos para hacer algo que creemos que es correcto. Es hora de volver a hacer algo grande, /b/.

Hablad entre vosotros, encontrad un lugar mejor para planearlo y luego llevad a cabo aquello que puede y debe hacerse.

Ha llegado el momento, /b/

Técnicamente —y los *geeks* hacen un hábito del hecho de sumergirse en especificidades técnicas—, una llamada a las armas llegó antes a 4chan, y también a 711chan (al parecer a las 18:11 h, según me dijeron). Sin embargo, éste parece haber sido el post que impulsó a tomar medidas al mayor número de trols. Si bien el ánimo general del hilo era de (exagerada) confianza y euforia, otros se mostraban comprensiblemente escépticos en cuanto a

enfrentarse —muchos menos eliminar— a esta organización tan extraordinariamente poderosa. Eran perfectamente conscientes de que colocar en el punto de mira a la Cienciología podía resultar (invocando la famosa serie de películas protagonizada por Tom Cruise) una “misión imposible”:

☐ Anonymous 01/15/08(Ma)19:46:35 No 51052578

misión imposible

un tablón de imágenes ocasional no puede acabar con una seudorreligión que cuenta con el respaldo de gente rica y un ejército de abogados.

incluso si todas las personas que UNA VEZ hayan navegado por /b/ se uniesen en una invasión masiva, aun seguiría siendo igual a nada.

además, si alguien fuese descubierto, ellos tendrían a 500 abogados pegados a su culo antes de que pudiesen pronunciar “litigio”.

los cienciólogos son famosos por acosar a los críticos.

¨anuncio 04/01/07(Vie)01:02:07 No.12345678

☐ Anonymous 01/15/08(Ma)19:50:22 No.51052862

»51052482
»51052578
No te involucres si no crees que es posible.

Al día siguiente, un mensaje premonitorio en /b/ lanzó el grito de guerra destinado a todas las actividades antiCienciología relacionadas con Anonymous reunidas bajo el eslógan “CHANOLOGY” y describía los futuros acontecimientos:

Archivo : 1200523664764.jpg-(22 KB, 251x328, 120046751294.jpg)



☐ **Anonymous** 01/16/08(Mié)17:47:44 No.51134054

El 15/1/08 comenzó la guerra.

El sitio de la Cienciología ya se encuentra bajo un intenso bombardeo y está cargando muy lentamente.

Pero esto es solamente la punta del iceberg, el primer asalto de los muchos que seguirán. Estamos obteniendo una victoria menor, pero sin el decidido apoyo de los chans, la Cienciología rechazará este ataque y quedará condenado a nada más que una entrada en la ED.

4chan, ¡responde a la llamada! ¡Únete a la legión contra la Cienciología, ayuda a su desaparición, a su largamente esperada extinción! Esta tiranía ha existido durante décadas, corrompiendo las mentes de los débiles; aunque hilarante, es bastante patética. Debemos destruir este mal y reemplazarlo por uno mayor - CHANOLOGY. Porque cuando salgamos victoriosos, los chans estarán unidos en un nuevo capítulo de existencia anónima y locura absoluta, habremos comenzado nuestra conquista del mundo. Si somos capaces de destruir la Cienciología, ¡podemos destruir todo lo que nos apetezca! El mundo no será otra cosa que nuestro juguete.

Haz lo correcto 4chan, conviértete no solo en una parte de esta guerra, sé una parte épica de ella. Al ser el mayor chan, tienes la llave de la mano de obra, lo que la legión necesita desesperadamente.

¡ADELANTE ANONYMOUS! UNIDOS, NOSOTROS, LA LEGIÓN, SOMOS IMPARABLES

tl;dr estamos eliminando la Cienciología, únete o lárgate.

No se permiten los Scifags en este hilo.

http://711chan.org/res/6541.html

Antes de que nadie pudiese decir “Ave, Xenu” (Xenu es el miserable, ruin extraterrestre señor de la galaxia, al menos según la versión cienciológica de la historia), estos trols —seguidos por mí poco después— se dirigieron a la red IRC Partyvan (un sitio de Anon) para ver cómo “estallaban” las celebraciones del troleo. O, al menos, así es como lo describió un participante en una charla a los estudiantes en una de mis clases en la universidad:

> La masa unida de anónimos colaboró a través de salas de chat para participar en diversas formas de cabronadas ultracoordinadas. Durante breves períodos entre el 15 y el 23 de enero, los sitios web de la Cienciología fueron hackeados y sometidos a la denegación del servicio compartido para expulsarlos de Internet. La línea directa del teléfono de Dianética recibió un abrumador bombardeo de llamadas falsas. Se enviaron por fax hojas de papel completamente negras a todos los números que pudimos encontrar. Y los “secretos” de su religión explotaron a lo largo y ancho de Internet. Yo también escaneé personalmente mi culo desnudo y se los envié por fax. Porque, que se jodan.

Al ver cómo esta incursión épica cobraba forma en tiempo real, me resultó fácil entender por qué los geeks y hackers que integran las filas de Anonymous colocaron a la Cienciología en su punto de mira: porque es su doble malvado. Yo no acabé por casualidad en este canal IRC, ya estaba inmersa en las tensiones culturales que existían entre geeks/internautas y cienciólogos. Un año antes había estado viviendo en Edmonton, una de las ciudades más frías de Canadá en (lo que parece) el confín de América del Norte. Estaba buscando y recopilando material en el archivo de categoría mundial sobre la Cienciología reunido por Stephen Kent, un profesor de Sociología en la Universidad de Alberta. Me dediqué a investigar una épica batalla librada entre geeks y la Iglesia de la Cienciología que se inició a comienzos de los años noventa y se prolongó durante dos décadas, comenzando después de que la Iglesia de la Cienciología apuntase a sus críticos, especialmente a aquellos que filtraban las escrituras secretas. Con el nombre humorístico de “Internet vs. Cienciología”, la batalla se libró tanto en la red como fuera de ella entre internautas —absolutamente comprometidos con la libertad de expresión– y la Iglesia de la Cienciología, absolutamente

decidida a eliminarla mediante todos los medios necesarios (legales o ilegales) con el fin de censurar las críticas e impedir que los documentos filtrados pudiesen circular por Internet. Yo había llegado a Edmonton con una hipótesis cultural bajo el brazo: los hackers y la Cienciología se encuentran en una relación diametralmente opuesta entre ellos. Eso no se debe solamente a que son diferentes, sino a que son exactamente diferentes. Son imágenes de espejo de cada uno, los complementos perfectos.

Examinemos la doctrina básica descrita en "Mantener a la Cienciología Funcionando", una publicación del Centro de Tecnología Religiosa de la Iglesia. La prosa actúa como un robot oxidado de primera generación que ha llegado tambaleándose a una esquina y, al descubrir que es incapaz de darse la vuelta, continúa avanzando con dificultad mientras repite monótonamente:

> UNO: TENER LA TECNOLOGÍA CORRECTA.
>
> DOS: CONOCER LA TECNOLOGÍA.
>
> TRES: CONOCERLA ES CORRECTO.
>
> CUATRO: ENSEÑAR CORRECTAMENTE LA TECNOLOGÍA CORRECTA.
>
> CINCO: APLICAR LA TECNOLOGÍA.
>
> SEIS: VER QUE LA TECNOLOGÍA SE APLICA CORRECTAMENTE.
>
> SIETE: RESOLVER LA EXISTENCIA DE TECNOLOGÍA INCORRECTA.
>
> OCHO: ELIMINAR LAS APLICACIONES INCORRECTAS.
>
> NUEVE: CERRAR LA PUERTA A CUALQUIER POSIBILIDAD DE UNA TECNOLOGÍA INCORRECTA.
>
> DIEZ: CERRAR LA PUERTA A LA APLICACIÓN INCORRECTA.

Al leer estas máximas en 2007 comprendí que cualquier hacker o geek que pusiera sus ojos sobre ellas se sentiría a la vez divertido y ofendido. Si la Cienciología está envuelta en secretismo, imbuida de dogma y subordinada al despliegue de la (pseudo) ciencia y la (falsa) tecnología para controlar a las

personas, hackear vidas a la luz de la exploración y el juego inquisitivo permite, y está permitido por, la ciencia y la tecnología. Los hackers dedican sus vidas y entregan sus almas para crear y programar las máquinas más sofisticadas del mundo. Son básicamente artesanos —motivados por un deseo de excelencia— pero aborrecen la idea de una única "tecnología correcta". De hecho, el hackeo es el lugar donde se combinan artesanía y astucia: fabricar una impresora en 3-D que imprime una impresora en 3-D; reunir un ejército de ordenadores zombies en un botnet y luego robar el botnet* de otro hacker para que el tuyo sea más poderoso; diseñar un robot con el único propósito de mezclar cócteles y exhibirlo en Roboexótica, un festival de robótica de cócteles que se celebra desde 1999; inventar un lenguaje de Programacion llamado Brainfuck ("jodecerebros") destinado a, bueno, sembrar el caos en la cabeza de cualquiera que intente programar con él. Creo que entiendes de qué va.

Una religión que reivindica un acceso privilegiado a la ciencia y la tecnología, al extremo de declarar que son «el único grupo en la Tierra que cuenta con una tecnología viable para abordar las reglas básicas de la propia existencia y poner orden en el caos»,[31] resulta profundamente ofensiva para los hackers, cuya única exigencia a la tecnología es que, como mínimo, debe realmente *hacer algo*, una tarea que ellos no dejan en manos de algún descubrimiento transcendental de la verdad sino, más bien, de su ingenio personal para descubrir soluciones a los problemas técnicos con la ayuda de consejos compartidos, intercambio de ideas y montones de códigos prestados.

De modo que tenía mucho sentido que Anonymous, un colectivo compuesto de geeks y hackers, se alzara contra la Cienciología. Pero había algo que no estaba claro: ¿estaba Anonymous troleando simplemente por su propia diversión en el terreno del lulz, o se trataba de una protesta seria? Aunque yo estaba bastante segura de que estos no eran actos deliberados de activismo, había claramente un ánimo político que se transmitía a través del IRC. La gente estaba innegablemente, y completamente, cabreada ante el hecho de que la Cienciología se atreviera a censurar un vídeo en "su" Internet y, sobre todo, uno tan desternillante. Anons estaban saturando de bromas telefónicas la línea directa de Dianética y enviando montones de pizzas sin pagar a los centros de la Iglesia, divulgando sus proezas en tiempo real a través de 4chan. Al principio, cualquier objetivo político parecía incidental. Y luego, semanas más tarde, un acto particular de "cabronada ultracoordinada" dio paso a una seria —aunque, indudablemente, irreverente— iniciativa de

carácter activista.

A medida que la popularidad de Chanology aumentaba, sus animados canales de IRC #xenu y #target se convirtieron en entornos de trabajo inadecuados para la proyección y los trucos publicitarios a los que aspiraban. Tres personas se marcharon y crearon el canal de IRC #press. Poco después creció para incluir a ocho miembros que trabajaron durante toda una noche hasta el amanecer para crear lo que aún hoy está considerada como la obra de arte más conocida de Anonymous. (Con el tiempo, el equipo aumentó su tamaño, #press se hizo caótico y sus miembros volvieron a separarse. Se llamaban a sí mismos *marblecake* [“bizcocho marmolado”], después de que uno de ellos encontrase la inspiración en el trozo de bizcocho que estaba comiendo.)

Si el vídeo de Tom Cruise tocó una fibra a la vez humorística e hiperbólica, este equipo se coordinó para crear un vídeo irónico cuyo carácter encarnaba una ambigüedad semejante al embaucamiento: divertido y serio, lúdico y siniestro a partes iguales. Para gran sorpresa de todo el mundo, el vídeo catapultó a Anonymous a un nuevo nivel de existencia.

En el vídeo, un monótono edificio corporativo de cristal se alza contra un fondo de nubes oscuras que cruzan amenazadoramente el cielo. Comienza un discurso que, si bien lo pronuncia una voz robótica, resulta poético e inspirador:

> Por el bien de vuestros seguidores, por el bien de la humanidad y para nuestra propia diversión, procederemos a expulsaros de Internet y desmantelaremos de manera sistemática la Iglesia de la Cienciología en su forma actual.
>
> Os reconocemos como un oponente serio y no esperamos que nuestra campaña se complete en un período breve. Sin embargo, no prevaleceréis para siempre contra las masas airadas del cuerpo político. Los métodos que elegís, vuestra hipocresía y la impunidad general de vuestra organización han firmado su sentencia de muerte. No tenéis donde esconderos porque estamos en todas partes. No tenéis ningún recurso en el ataque porque por cada uno de nosotros que caiga, otros diez ocuparán su lugar.
>
> Somos conscientes de que muchos denunciarán nuestros métodos como

> similares a los que emplea la Iglesia de la Cienciología, aquellos que afirman la obvia verdad de que vuestra organización utilizará las acciones de Anonymous como un ejemplo de la persecución de la que, durante tanto tiempo, habéis advertido a vuestros seguidores; esto es aceptable para Anonymous. De hecho, es alentador.

Era una declaración sincera, pero sinceramente una broma. Estas imágenes poéticas sobre un levantamiento eran retóricas, pero era un mensaje tan convincente, tan atractivo como una dirección propia del lulz que atrapó a los trols de Anonymous en un esfuerzo por desmantelar sistemáticamente a la Cienciología. Quedaron atrapados —como tantos embaucadores antes que ellos— en su propia trampa embaucadora. Anonymous, con su súbita participación en la política del lulz, dio origen a los vilipendiados moralfags y líderfags. Estos Anons —contaminados, de alguna manera, por un gusto accidental por la justicia— catalizaron efectivamente uno de los movimientos de protesta más potentes de nuestros tiempos.

La accidental cadena de acontecimientos se desarrolló de esta manera: el vídeo suscitó de manera inesperada un debate sobre si Anons debía salir a las calles a protestar contra la Iglesia de la Cienciología o bien permanecer fiel a sus delirantes raíces y continuar con el lulz y sus incursiones en la red. El momento ayudó a tomar la decisión por ellos, inclinando la balanza en favor de las manifestaciones callejeras. Gregg Housh, uno de los editores del vídeo y miembro original de *marblecake*, lo explicó de esta manera en el curso de una entrevista: «Había gente que pensaba que Anonymous o 4chan no debían tomar las calles, pero el consenso para hacerlo se produjo de una manera relativamente fácil después del vídeo. Parecía enormemente oportuno, el vídeo adecuado en el momento adecuado.»

Aunque los Anons optaran por la protesta callejera, no querían abandonar completamente el troleo; en cambio, su intención era ampliar su repertorio. Un Anon en el IRC reflejó todo el espectro —legal, ilegal, hilarante, serio— que estas hordas de trols ocupaban cada vez más (o querían ocupar) entre mediados de enero de 2008 y la primera protesta callejera (su seudónimo había sido cambiado):

> <Lulamania>: El escenario final: llamada falsa + DDoS de Anonymous, gobiernos estadounidense y francés renuevan cargos por fraude, evasiones fiscales y actividades ilegales, los pastores locales de la Iglesia

revelan a su congregación los males de la Cienciología, ex miembros y familias son entrevistados en TV sobre su experiencia, grupos de activistas llevan a cabo incursiones y protestas autorizadas y las noticias cubren todo lo anterior...

<Lulamania>: No olvidar que ésta es una guerra de desgaste. No podemos provocar la quiebra de la Iglesia de la Cienciología directamente, se trata de conseguir la atención de los medios de comunicación, informar al público, agotar a sus miembros, desactivar sus servicios informáticos y telefónicos, combatir el lavado de cerebro de sus reclutas potenciales, y por el lulz.

El 24 de enero de 2008, Anonymous anunció que el 10 de febrero sería un día de protesta. Pocos días después de esta primera llamada a la acción, Mark Bunker, el crítico de la Cienciología, aprovechó este momento de alto voltaje y presionó para que se empleasen solo tácticas legales. Al igual que Eshu, el embaucador arquetípico de la comunicación y las encrucijadas, se dirigió a los trols mediante un vídeo (¡sagrado Xenu!), les elogió (inteligente) y les pidió que se unieran a la causa (¡sagrado Xenu!). Su mensaje tenía la intención de que la sangre no llegase al río que reinara el lulz, y «por favor, por favor, por favor abstenerse de cualquier cosa que sea directamente ilegal». En un extenso post a un foro en whyweprotest.net, Bunker explicó qué era lo que le había llevado a hacer ese vídeo: «Después de haber visto el 'Mensaje a la Cienciología' de Anonymous, me preocupaba haber ayudado a generar ataques que pudieran asustar a los miembros del personal de la Cienciología y también causar problemas legales a los miembros de Anonymous, de modo que decidí que necesitaba hacer esa grabación inicial para Anonymous.»[32]

Aunque muchos ya habían estado pensando en esta dirección, no todos estaban de acuerdo con la visión que ofrecía este tío cincuentón, robusto y con aspecto de oso a quien Anonymous rebautizó "Wise Beard Man" (barbudo sabio) por su pose erudita y vello facial blanco. (Apenas unos años más tarde aparecerían nuevas redes de activistas que adoptaron tácticas militantes e ilegales como el DDoS, no para trolear sino para manifestar su disidencia política.) Sin embargo, un número considerable de ellos cambió de rumbo y tomó el camino del activismo militante; los argumentos esgrimidos por Bunker empujaron a Anonymous a emplear tácticas legales (en su mayor parte) en sus primeras manifestaciones importantes.

El *marblecake*, actuando en gran medida en secreto (una cohorte de no iniciados sabía de su existencia), era consciente de que la gran mayoría de participantes potenciales estaba constituida probablemente por neófitos en las protestas. Si estos nerds, geeks, hackers y trols de Internet aparecían en masa para protestar sin tener ninguna experiencia previa en el campo del activismo sería sin duda una receta abocada al desastre. De modo que tenían que aprender lo más rápidamente posible. Les proporcionaron un curso intensivo sobre la mecánica, los desafíos y los componentes propios de una protesta pacífica en un vídeo llamado "Código de Conducta".[33] Colgado el 1 de febrero de 2008, una voz robótica enumera veintidós reglas. No se ignora ningún detalle: el vídeo les recuerda a los participantes que deben llevar calzado cómodo, beber mucha agua, guardarse para sí en Internet las bromas que sean particularmente desagradables y frikis (porque podrían ofender a los espectadores), abstenerse de cualquier forma de violencia, obtener los permisos necesarios, utilizar eslóganes pegadizos y grabar el evento. Puesto que *marblecake* sabía que los cienciólogos utilizarían todos los medios a su alcance —incluidas fotografías en alta definición— para identificar y posteriormente acosar a los manifestantes, una de las reglas exhortaba a los participantes a cubrirse el rostro, pero señalaba, en una declaración que ahora resulta irónica, que no había necesidad de usar máscaras: «Regla No.17: Cubre tu rostro. Esto impedirá que te identifiquen en los vídeos grabados por los hostiles, otros manifestantes o la seguridad. Usa pañuelos, sombreros y gafas de sol. Las máscaras no son necesarias y llevarlas en el contexto de una manifestación pública está prohibido en algunas jurisdicciones.»

Necesarias o no, cuando miles de Anons y partidarios invadieron las calles en ciudades de todo el mundo, las máscaras aparecieron en todas partes. Para entonces, la máscara de Guy Fawkes se había convertido en un icono cultural pop gracias a la exitosa película de Hollywood *V de Vendetta*. La película presenta a un solitario anarquista en su lucha contra un estadio orwelliano y distópico. La máscara también había aparecido antes en 4chan, utilizada por un amado personaje meme con una clara tendencia al fracaso: Epic Fail Guy. Muy conocida, fácil de comprar e imbuida de una innegable energía simbólica —tanto debido a su historia como a su iteración más reciente—, la máscara de Guy Fawkes se convirtió en la máscara del día para disuadir las miradas indiscretas de la Cienciología. Más tarde funcionaría como la firma icónica de Anonymous.

Los acontecimientos de aquel día oscilaron entre la protesta política y las

tonterías carnavalescas. ¿Por qué participó tanta gente? Durante un chat informal, un antiguo Anon y miembro de *marblecake* me explicó (correctamente, creo) que «escuchar [sobre] los primeros informes de las protestas de los australianos orientales el 10 de febrero de 2008, realmente puso las cosas en marcha... Si esas protestas no se hubiesen materializado, me imagino que la concurrencia en otras ciudades no habría sido tan importante». Mientras gran parte del mundo occidental dormitaba, en Australia se lanzaron a la calle entre 550 y 850 manifestantes, transmitiendo sus cifras a otros en fotografías y vídeoclips en tiempo real, provocando un efecto dominó que se hizo sentir en todo el mundo occidental. En Londres, la multitud alcanzó hasta seiscientas personas y este número fue igualado en Norteamérica, donde los manifestantes ocuparon las calles en ciudades pequeñas en el centro del país y en importantes urbes metropolitanas como Los Ángeles, donde la asistencia fue de un millar de personas.

Seis meses después de que una emisora local de Fox News etiquetara a Anonymous como “la Máquina del Odio de Internet”, el colectivo tenía legiones de partidarios en las calles —no solamente geeks y hackers martilleando sus teclados— que aprovechaban el nombre del grupo, su ética del anonimato y la variada iconografía concomitante. Aquella tarde se pudo ver en los canales de noticias por cable a hombres y mujeres que llevaban máscaras de Guy Fawkes y trajes negros y alzaban pancartas que rezaban «Nosotros somos Internet».

Si bien ésta puede haber sido la primera vez que Anonymous se manifestaba en las calles congregando a un gran número de partidarios, las campañas de troleo previas exhibían un atractivo cuasi activista. Por ejemplo, en 2007 Anonymous colocó en el punto de mira a Hal Turner, una personalidad de derechas de las ondas radiofónicas, no solamente por el lulz (y la venganza) sino también por “racista”. Anonymous ya se había centrado en él en 2006 con una serie de bromas telefónicas y ciberataques que dejó inactivo su sitio web. Hal Turner contraatacó publicando los números de los bromistas telefónicos y provocando con esta respuesta que Anonymous asestara un duro golpe al corazón de su imperio radiofónico, volviéndolo loco con hackeos y troleos incesantes. El siguiente post en un blog, colgado por un participante de Anonymous antes de la segunda ronda de incursiones, transmite la innegable sensibilidad política que motivaba la acción:

Aquellos de vosotros que pasáis algún tiempo en los sitios de troleo de

> Internet, tales como 4chan, 7chan, YTMND, etc., sin duda ya conoceréis esta noticia, pero merece la pena repetirla.
>
> Hal Turner es, en pocas palabras, un Nazi [*sic*]. Un Nazi con su propio programa de radio. Lamentablemente para él, tampoco ha conseguido una audiencia masiva, excepto por los /b/tardos y otros diversos trols que decidieron arruinar totalmente su vida en línea. Tal como muestra un vídeoclip de Fox News abajo [*sic*] sobre él promoviendo el asesinato de un juez estadounidense, no es exactamente alguien por quien debamos sentir lástima.[34]

Chanology se diferenciaba de estas incursiones anteriores por un aspecto fundamental: se convirtió en un elemento permanente en el panorama político. En las semanas y los meses que siguieron a las primeras manifestaciones callejeras, Chanology continuó protestando contra la incesante campaña legal y extralegal de la Cienciología dirigida hacia los críticos y todos aquellos que se atrevían a revelar o hacer circular documentos internos de la Iglesia. Tal como me explicó un manifestante durante una protesta callejera en Irlanda: «Vine por el lulz; me quedé por una mayor justicia, una victoria épica y el moar lulz.**» ¿Pero por qué? ¿Cómo hizo para organizarse un colectivo tan caótico? Y ¿podría seguir prosperando el lulz cuando buscara justicia?

Por qué (y cómo) protestamos

Cada vez que reflexiono acerca de la constitución y la perseverancia de Chanology me impresiona como un milagro menor en los anales de la resistencia política. No hay duda de que un subgrupo de troleo (como las incursiones a Hal Turner) toca una fibra política, pero la energía que existe detrás de estas primeras incursiones tiende a disiparse pocos días o semanas después. Chanology se sustentaba en un entorno no exactamente propicio para una organización política consciente a largo plazo; es conveniente que consideremos la dinámica social detrás del éxito de Chanology, especialmente a la luz de las numerosas tensiones —por ejemplo, entre las acciones motivadas por el lulz y los objetivos morales— que la afectaron desde el comienzo.

Para empezar, la formación de una voluntad política sostenida estaba

garantizada por la amplia cobertura que las manifestaciones callejeras de febrero habían tenido en los medios de comunicación. Desde el primer día, la gente que llevaba máscaras de Guy Fawkes ocupó las portadas de todos los telediarios. Centenares de fotografías y docenas de vídeos caseros de las protestas locales se compartieron a través del IRC y de sitios web populares de las redes sociales como Digg, Myspace, Yahoo! Groups y LiveJournal. Para muchos Anons, las representaciones externas validaban el Proyecto Chanology y a Anonymous. Esta dinámica de éxito y amplificación del fenómeno se repetiría en numerosas oportunidades a lo largo de la historia de la organización.

Los motivos ulteriores también tuvieron una gran importancia: si bien el activismo era un factor significativo para muchos Anons (y el lulz siempre resultaba atractivo), muchos se echaron a la calle por la rara oportunidad de conocer a algunos de sus hermanos de Anonymous. Algunos se quedaron, otros regresaron a los rincones oscuros de Internet y rebatieron esta sensibilidad política incipiente, en ocasiones ridiculizando a sus compañeros como moralfags e intensificando sus actividades de troleo, llegando incluso a tener al propio Chanology como una fuente de lulz. Tomemos, por ejemplo, la siguiente propuesta —un llamamiento para recuperar Anonymous de los moralfags con el propósito de resucitar la Máquina del Odio de Internet— formulada en la muy activa plaza virtual de Chanology, el foro web Enturbulation.org (que finalmente fue adaptado a WhyWeProtest):

> Compañeros hermanos y hermanas,
>
> Hace seis meses iniciamos una yihad para asegurar que nuestras comunicaciones por Internet estuviesen libres de mariconerías. Se llamó a las armas y respondimos como una legión. Hoy, cuando miramos retrospectivamente nuestros ingenuos esfuerzos resulta obvio que nos han robado aquello que por derecho nos pertenece.
>
> Nuestro nombre, nuestros memes y nuestros esfuerzos han sido secuestrados por gente que no entiende y no se da cuenta de que nuestra fuerza procede de la diversidad, la indiferencia y la constancia. Aunque normalmente esto no habría sido un problema, aquellos que han permanecido en las trincheras protegiendo nuestros ideales se encuentran ahora en un punto muerto.

> Necesitamos vuestra ayuda, estoy de rodillas [*sic*] pidiendo que aquellos que han abandonado el Proyecto Chanology regresen y lo recuperen. Volved a traer el lulz, la máquina del odio, no permitáis que algunos detractores bastante poderosos influyan sobre vosotros.
>
> Comenzamos esto para asegurar que nuestras comunicaciones por Internet estuvieran libres de la tiranía y, aunque estoy de acuerdo en que hay batallas futuras que tal vez sean más importantes para este fin, ésta es la primera de ellas. Modelamos a los newfags en trols templados y nos aseguramos de que cuando el hombre venga a reclamar lo que es legítimamente libre, todos estemos preparados para asegurar que eso no ocurra.
>
> A lo largo de las próximas semanas veréis viejos rostros que atacan vuestros canales, vuestros tablones, vuestros IRC para asegurar que Anonymous retiene lo que es nuestro. Recuperad Chanology de una vez por todas, quemad hasta los cimientos cualquier cosa que se nos oponga.[35]

La oposición binaria entre moralfags y buscadores del lulz "solidificados" era, y aún es, menos inequívoca de lo que sugiere este post. En los canales de IRC dedicados a la organización política, una minoría pequeña pero bastante ruidosa ofrecía asistencia técnica en busca de beneficios políticos al tiempo que insistía también en llevar a cabo acciones de lulz, incluidas formas horrendas de troleo. Entre estos trols destacó un individuo llamado CPU (nombre ficticio). Ampliamente considerado como un talentoso hacker, CPU ofreció desinteresadamente su asistencia técnica. Pero también era un crítico feroz de los moralfags y reclamaba a gritos formas de troleo realmente crueles. Por ejemplo: el 16 de marzo de 2008, CPU sugirió lo siguiente en el canal de IRC #internethatemachine, una sala de chat para criticar a los moralfags (todos los nombres han sido cambiados):

> <CPU>: Internethatemachine es para esos enfermos de los moralfags y los lovefags ¿estoy en lo cierto lol?
> <CPU>: Debemos atacar un foro al azar por el lulz. ¿Alguien recuerda las incursiones de emetofobia?
> <CPU>: estoy buscando un foro lol.
> <CPU>: oh lol http://www.suicideforum.com/

<CPU>: ¿La primera persona que empuje a alguien hasta el límite gana?
<CPU>: ¿Quién recuerda a los felices amigos de los árboles? :p
<CPU>: Destrozamos los foros cada día durante aproximadamente 2 semanas lol.
<CPU>: Al final hicimos polvo a Emo-corner, duro pero llevó tiempo.
<CPU>: Un montón de personas atacando al mismo cabroncete al mismo tiempo lol.
<CPU>: Les quitamos su foro al menos dos veces y añadimos una página desfigurada lol.
<CPU>: ¿O podríamos encontrar un foro sobre epilepsia y llenarlo de correo basura con regalos con luces brillantes o algo por estilo?
<XB>: http://www.epilepsyforum.org.uk/
<CPU>: adelanteadelanteadelante
<CO>: ¿Oh dios...phpbb*** también? :D Oh es tan explotable.
<CPU>: ¿Cambiar la página principal por una cosa grande y brillante?
<CPU>: lol creando una cuenta ahora:D
<CPU>: Si podemos cambiar la página principal utilizamos esta http://www.freetheflash.com/flash/epilepsy-test.php

No se sabe a ciencia cierta si CPU y el resto de participantes en el canal llevaron a cabo realmente esta campaña, pero alguien lo hizo. El 22 de marzo de 2012, los trols participaron en uno de los ataques más famosos y moralmente reprobables conocidos hasta la fecha, invadiendo un foro sobre la epilepsia y colgando imágenes brillantes e intermitentes que provocaron ataques a algunos de sus miembros. Casi todas las informaciones atribuyeron erróneamente el ataque a Anonymous en su lucha contra la Cienciología, que no era probablemente el caso; varios hilos en diferentes tablones de imágenes culparon de esta acción a otro célebre tablón infestado con trols: eBaum's World. Si bien Chanology no estaba detrás del ataque, la incursión dejó una mancha oscura en el nombre de Anonymous y enfureció a algunos miembros de Chanology.[36]

Cabe señalar que si bien los cruzados antiCienciología estaban mortificados por el ataque al foro sobre la epilepsia, estos moralfags incipientes no renegaron completamente de esa desviación o del lulz. Después de todo forma parte del tejido de su cultura. En cambio, Chanology se introdujo en una clase de lulz más ligero y amable. Por ejemplo, la ciudad de Nueva York es la sede de una manifestación zombie relámpago anual (y bastante considerable) en la que alrededor de un millar de cuerpos macabros, ensangrentados, quejumbrosos y de movimientos lentos se arrastran (o, en ocasiones, se desplazan en patines) por las calles de la ciudad. Los organizadores de Chanology en Nueva York pensaron que podía resultar

divertido que esta muchedumbre zombie desfilara delante de la Iglesia de la Cienciología el día en el que Anonymous realiza su protesta mensual en ese lugar. La multitud zombie aceptó encantada. Los zombies iniciaron su paseo recorriendo a cámara lenta la calle 46, profiriendo obscenidades contra la Iglesia de la Cienciología mientras los manifestantes de Chanology humillaban y se mofaban de la Iglesia, obviamente orgullosos del lulz teatral (y mayormente prohibido para menores) que habían conseguido montar.

Pero no existe mejor ejemplo de la participación activista de Anons teñida de humor carnavalesco que la Operación Slickpubes en enero de 2009, organizada también por la célula del Proyecto Chanology en Nueva York. El acto consistió en que una persona casi desnuda (el hombre se había untado parcialmente por una capa de vaselina mezclada con vello púbico) entrase en una edificio de la Iglesia de la Cienciología. El objetivo de esta iniciativa pasada de rosca no era simplemente oponerse y enfurecer a los miembros de la Iglesia a través de un acto humillante (aunque sin duda formaba parte de la acción), sino revitalizar también aquello que algunos participantes consideraban el espíritu tambaleante del lulz. Las fuerzas de Apolo tenían que equilibrarse, eternamente, con una pizca de rebeldía dionisíaca embaucadora. Más tarde, los miembros de Chanology escribieron sobre este incidente en un post colgado en un blog en motherfuckery.org, un sitio diseñado para conmemorar sus orígenes:

> Lo que ocurrió en los meses siguientes sólo podría describirse como “lulz” y “u mad”, cuando la grabación de la operación Slickpubes completó sus rondas en el mundo de Chanology, Anonymous y los rangos superiores de la Cienciología. Los que pensaban que Chanology era demasiado sumisa se alegraron.[37]

Con este emergente Anonymous, orientado políticamente, el lulz se desplegaba con frecuencia, como sucedió con la Operación Slickpubes, de un modo jocoso y dionisíaco: atrevido pero también arriesgado. Trabajaban haciendo que uno se riera a carcajadas y se estremeciera a la vez y ofrecían también una política de la subversión. Pero no sin que eso acarrease consecuencias. De hecho, en el caso de la Operación Slickpubes, el nudista embadurnado fue arrestado por su gamberrada. El incidente también provocó que el Departamento de Policía de Nueva York comenzara a vigilar secretamente a Anonymous (un bautismo necesario para cualquier grupo

político nuevo y ¿qué mejor manera que atraer a las fuerzas de la ley que hacerlo a través del vello púbico?).[38] Es posible que Wise Beard Man haya amansado al embaucador de Anonymous, pero no consiguió eliminar totalmente su espíritu travieso.

La voluntad de Anonymous de causar estragos en busca del lulz y la libre expresión (y en oposición a la conducta indebida y el engaño exhibidos por la Iglesia de la Cienciología) recuerda a los "bandidos sociales" europeos del siglo XIX descritos por el historiador Eric Hobsbawm en su libro de 1959 *Rebeldes primitivos*. Estos bandidos son miembros de mafias, sociedades secretas, sectas religiosas, turbas urbanas y bandas de delincuentes; son, en definitiva, matones pero, según Hobsbawm, alimentan un ligero espíritu revolucionario: parte de su botín es habitualmente redistribuido entre los pobres, a quienes además protegen de otros bandidos. Hobsbawm define a los bandidos como figuras «prepolíticas» y «que aún no han encontrado, o apenas han comenzado a encontrar, un lenguaje específico con el cual expresar sus aspiraciones sobre el mundo».[39] Anonymous ha trabajado para encontrar ese lenguaje con notable celeridad desde que lanzara el Proyecto Chanology.

Esas gamberradas contrastan, sin embargo, con la narrativa moral de Hobsbawm, según la cual los bandidos solo pueden convertirse en actores políticos viables si renuncian a sus tácticas amenazadoras y aceptan las formas de poder convencionales. Para Hobsbawm, el bandido se enfrenta a «las fuerzas de la nueva sociedad que es incapaz de entender. Como máximo puede luchar contra ella e intentar destruirla». Esto explica por qué «a menudo el bandido es destructivo y salvaje más allá del ámbito de su mito».[40] Los bandidos digitales de la actualidad, sin embargo, entienden perfectamente las fuerzas de la creación destructiva, desplegándolas de manera consciente con una intencionalidad política.

El lulz conservaba un lugar prominente pero no ocupaba la cabecera de la mesa. Chanology estaba muy lejos de la caótica horda de chalados. Mientras actuaban en medio de un a menudo contaminado entorno de tragedia, luchas intestinas y grupos dispares, los miembros de Chanology desarrollaron una sólida organización, con participantes clave que dedicaban un tiempo extraordinario a este esfuerzo. Podemos tomar, como caso de estudio, el software que hay detrás del inmensamente popular foro de la web Why We Protest, escrito en su mayor parte por un joven geek francés llamado Ravel. Describió su adscripción a Chanology como un encaje natural, teniendo en cuenta que él había tenido «algunos años traviesos y fuertes

afinidades con las culturas del hacker y de la libre expresión. Cuando se produjo la llamada a la acción no lo dudé un instante y dije ‘vamos a hacerlo’».[41] Durante los seis años siguientes, y todavía hasta hoy, se convirtió en el proyecto de su vida.

El proyecto surgió de la creación del #website IRC channel. A Ravel (conocido como Sue) no le gustaban las propuestas existentes y, en el clásico estilo hacker, comenzó a codificar el software según su propia visión con la ayuda de otros dos programadores. Debido a este intenso trabajo fue contactado para que formase parte de *marblecake*:

> Se pusieron en contacto conmigo y pasé a formar parte del (indebidamente) famoso colectivo *marblecake*... Hasta la fecha ha sido el grupo más organizado con el que he colaborado en la red. No estaría exagerando cuando digo que el cuórum de participantes dedicaba más de 70 horas por semana a proyectos relacionados con los medios de comunicación, planificando, abordando cuestiones de comunicación y en sesiones de intercambio de ideas. Cumplía a la vez funciones de centro de estudios y de estudio de producción. Las reuniones se celebraban casi cada día, se realizaban evaluaciones, se conservaban las actas, etc.[42]

«¿Qué coño es *marblecake*?»: Primeros desafíos al nuevo Anonymous

Con una considerable porción de Anons que ahora participaba de manera inequívoca en este estilo de hackeo políticamente comprometido (complementado con una estructura técnica compuesta de canales, encuentros mensuales en los actos convocados por Chanology y una emergente variedad de memes y objetos específicos del activismo de Anonymous, como las máscaras de Guy Fawkes), era solo una cuestión de tiempo que esta identidad se fracturase. La homeostasis no es, precisamente, el estado preferido de Anonymous, sin duda no antes de Chanology y, definitivamente, no después de ese proyecto.

Detengámonos un momento en la caracterización de *marblecake* hecha por Ravel como «el grupo más organizado con el que he colaborado online». Sin lugar a dudas, *marblecake* era extremadamente eficaz en la tarea de crear propaganda, publicar notas de prensa, negociar entre las diferentes células

repartidas por la ciudad y sugerir temas para las protestas mensuales. Entre otros factores, muchos atribuyeron su éxito a una cualificada organizadora que había adoptado el nombre de darr. Un colega me la describió como «resuelta y tenaz, amable y comprensiva», unas cualidades que Anon consideraba cruciales para los logros de *marblecake*.

Pero entonces darr cometió el error de intentar impulsar una propuesta impopular. Para la protesta de mayo de 2008, *marblecake* sugirió el tema “Operación Psychout” para exponer los abusos en materia de derechos humanos cometidos por la Cienciología en el campo de la psiquiatría, que «fue recibido con una gran oposición», según me explicó un miembro activo del grupo. Poco después, *marblecake* colocó el último clavo en su propio ataúd —al menos en la forma en la que existía en aquella época— al intentar “imponer” la propuesta, lo que llevó a los miembros de Chanology a “desembarazarse de darr”, a quien se veía como una partidaria particularmente descarada. O una “aspirante a líderfag sedienta de poder”, en palabras de un Anon. Los trols, sobre todo, se le lanzaron a la yugular, sometiéndola a un intenso doxeo y divulgando mentiras. Ella abandonó el proyecto y se le perdió la pista.

Marblecake existía en una zona nebulosa. Cuando los ocho miembros se separaron en enero de 2008 dejaron una notificación permanente en el canal de chat #press: «¿Quieres tener acceso adonde está toda la acción? Mueve tu culo a SSL y no seas maricón; D—Tema colgado por darr el 16/02/2008.» Aquellos que se sentían intrigados por este seductor mensaje podían preguntarle por él a un oldfag —alguien que había estado presente desde el principio— para que les guiase por los distintos pasos para instalar Encryption (SSL). También tenían que estar dispuestos a dedicarle muchas horas al asunto. De este modo, *marblecake* creció hasta incluir a veinticinco participantes. Finalmente, el mensaje fue sustituido, el crecimiento se estancó y los recién llegados ignoraban por completo su existencia.

Tres meses después de la salida de darr alguien colgó un mensaje en Why We Protest: «¿Qué coño es *marblecake*?» La respuesta que recibió informaba efectivamente a un grupo mucho más numeroso de Anons acerca del proyecto semisecreto. Para muchos, la respuesta reveló por primera vez que, bajo el manto de Chanology, se habían desarrollado múltiples facciones:

Estoy en *marblecake*, y no tengo ningún interés en ser un líderfag.

> Me gusta contestar preguntas.
>
> La historia resumida es, es/era un pequeño centro de estudios que producía noticias de forma anónima y secreta. El lado positivo sería que ha “sufrido por su propio éxito”—produce suficientes noticias importantes que desea que permanezcan completamente secretas... y produciendo suficientes noticias para que el resto de Anonymous tomara conciencia —en diversos grados— de que existe una camarilla secreta de anons que trata de manipular las cosas entre bastidores.
>
> El lado negativo es... que existe una camarilla secreta de anons que trata de manipular las cosas entre bastidores. Y existen fundadas razones para creer que se les subió el éxito a la cabeza demasiado pronto. Ellos produjeron el vídeo original del “mensaje a la cienciología” (mucho antes de que yo me implicase). Ellos también estaban dirigidos por Darr, quien cabreó a las personas equivocadas, tenía una actitud equivocada y generalmente no manejaba bien las críticas.
>
> [...]
>
> En cuanto a las facciones, están *marblecake*, enturbmods, OCMB (siglas de *Operation Clambake Message Board*) y los canales de #enturbulation (además de cada célula individual de la ciudad y probablemente muchas otras que no conozco). *Marblecake* y enturbmods se han peleado, #enturbulation (específicamente Tuesday y WB) se han enfrentado a *marblecake*. A menudo OCMB ha tenido problemas con enturbulation. #enturbulation generalmente odia a *marblecake*. Son un montón de luchas internas estúpidas y mucha gente ha estado involucrada con más de uno de esos grupos. Y nadie debería sentirse “excluido” por no participar en ninguno de ellos, porque todos son básicamente conserjes de los *verdaderos* anons, los que salen a las calles en las ciudades repartiendo flyers y formando piquetes.[43]

El hilo siguiente fue largo y amargo. Algunas personas estaban furiosas, incluidos algunos miembros y ex miembros de la camarilla. Después de este alboroto, *marblecake* naufragó durante algún tiempo antes de experimentar lo que un Anon llamó una “reforma”. A partir de entonces comenzaron a

funcionar con mayor transparencia con respecto a su función como “coreógrafos”, tomando prestada la expresión utilizada por Paolo Gerbaudo para describir un estilo de liderazgo común entre los movimientos de protesta globales de 2011.[44]

La salida de escena de *marblecake* puso de manifiesto que una simple oposición binaria entre líderes y seguidores no conseguía recoger la compleja dinámica organizativa en un medio tan abocado a la descentralización. Anonymous no es un frente unido sino una hidra que incluye numerosas redes diferentes. Incluso cuando se aborda un único proyecto, hay grupos de trabajo que a menudo están enfrentados entre sí, por no mencionar, en términos más generales, las guerras civiles libradas entre los diferentes nodos de Anonymous. Pero aun cuando los Anons no siempre estén de acuerdo con todo lo que se hace bajo los auspicios de Anonymous, tienden a respetar el hecho de que cualquiera puede asumir el nombre. La máscara, que se ha convertido en su firma icónica, funciona como una baliza eterna, transmitiendo el valor simbólico de la igualdad, incluso frente a las amargas divisiones y desigualdades. Naturalmente, a pesar de la ausencia de una jerarquía estable o de un único punto de control, algunos Anons son más activos e influyentes que otros, al menos durante períodos limitados. Anonymous se ciñe a una variedad particular de lo que los geeks llaman “doocracia”, con individuos motivados (o aquellos que tienen tiempo libre) para ampliar su arquitectura en red que contribuyen con tiempo, trabajo y atención a los esfuerzos existentes, o que dejan que sean otros los que inician sus propios proyectos, mejor alineados con sus ideales y principios.

Un punto muy importante es si un movimiento admite la existencia de líderes blandos. Este hecho se relaciona con otra cuestión que afecta a muchos movimientos sociales: ¿Cómo mantiene un movimiento social la suficiente permeabilidad para que los recién llegados puedan incorporarse a grupos preexistentes cuya tendencia es convertirse en camarillas? Sin un reconocimiento explícito de la existencia de liderazgo, un proyecto puede caer con facilidad en la “tiranía de la falta de estructura”, una situación mediante la cual la manifestación de una ideología descentralizadora funciona como una trivialidad que oscurece o reorienta la atención lejos de los nodos de poder firmemente arraigados pero ocultos que actúan entre bastidores.[45]

Como consecuencia de la acalorada controversia que estalló en Why We Protest, muchos Anons aceptaron que *marblecake* desempeñaba un papel organizativo muy valioso. El blando liderazgo del grupo dio lugar a una

organización impresionante, tanto en la red como en muchas ciudades. Pero el consenso general se inclinaba hacia una mayor transparencia.

«No hay manera de que la Cienciología pueda derrotarnos más. Se acabó.»

En 2014, el Proyecto Chanology es ya una sombra de lo que fue. Ahora las protestas mensuales atraen solo al núcleo duro del grupo, con una concurrencia entre pequeña y mediana en unas pocas ciudades (como Dublín, Düsseldorf, Hamburgo y Nueva York). No obstante, esta situación refleja no solo el fracaso, sino el éxito. Si bien el Proyecto Chanology no destruyó la Iglesia de la Cienciología, consiguió alterar el juego de un modo tan profundo que ahora sus críticos no podían dejar de temer las represalias. La Iglesia ya no dominaba la situación.

Este punto fue explicado claramente por numerosos ex miembros de la Cienciología durante una conferencia a la que asistí el 30 de junio de 2012 llamada Dublin Offlines, organizada por ex cienciólogos. Habían transcurrido poco más de cuatro años desde que este dudoso elixir fermentase por primera vez a través de una extraña mezcla de ex miembros de la Iglesia, críticos de la Cienciología y arrogantes geeks de Internet. Esta ocasión parecía el momento y lugar oportunos para que yo hiciera balance de la importancia histórica del proyecto.

La conferencia se celebró en el Teacher's Club (conocido también como Club na Múinteoirí) de Dublín, ubicado en un edificio de estilo georgiano de cuatro plantas que ofrecía un refugio íntimo y acogedor de la omnipresente llovizna irlandesa. Al evento asistieron alrededor de setenta personas, una porción considerable de ellos con el rostro cubierto con máscaras de Guy Fawkes. En consonancia con la teatralidad habitual de las manifestaciones callejeras, algunos Anons llegados de Francia se veían muy elegantes con sus disfraces de circo y pantomima. Dos de ellos iban disfrazados de duendes gigantes. Mi favorito era un tío que llevaba un disfraz de vaca.

Los oradores incluían a ex cienciólogos del barco de la Iglesia, algunos de la Sea Org (una orden religiosa hermana no incorporada e integrada por los miembros más comprometidos de la Iglesia), Gerry Armstrong (el ex secretario personal de L. Ron Hubbard), Jamie DeWolf (el bisnieto de L. Ron Hubbard), un par de académicos (yo incluida) y un puñado de personas que

habían perdido a sus familiares a causa de la Iglesia. El maestro de ceremonias era Pete Griffiths, un dublinés ex director ejecutivo de Kendal Mission, en Cumbria, Inglaterra, con un traje brillante plateado que hacía juego con su enérgica personalidad.

Como me alojaba en la otra punta de la ciudad llegué un poco tarde y el ambiente ya estaba bastante animado. Entré de puntillas, saludé en silencio con la mano a algunas de las personas que había conocido en un viaje anterior a Dublín y me deslicé a mi asiento. Me sentía bien aunque muy baja de cafeína. Al acabar el día, después de haberme revuelto inquieta en mi silla durante muchas de las intervenciones, estaba emocionalmente agotada. Los ex cienciólogos aportaron conmovedores relatos personales del poder del culto para estrangular las vidas de los que están en la Iglesia y de aquellos que se atreven a abandonarla. La política de la Iglesia de la Cienciología ordena que los nuevos reclutas corten todos los lazos con cualquier miembro de su familia o amigo que se opongan a su decisión (como hacen muchos de ellos); abandonar la organización representa a menudo una pesadilla logística, ya que la red personal de esa persona ha sido completamente eviscerada. Si un miembro hace pública su marcha de la Iglesia queda marcado bajo la "política del juego limpio", que establece que la persona «puede ser privada de sus bienes o dañada por cualquier medio por cualquier cienciólogo sin ningún castigo para el cienciólogo. Puede ser seducida, demandada, engañada o destruida».[46]

La intervención de Tory Christman destacó de entre las demás. Antes de abandonar la Iglesia el 20 de julio de 2000 había sido cienciólogа durante treinta y un años, período durante el cual perfeccionó sus habilidades oratorias como encargada de las relaciones públicas de la Iglesia. Christman se mostró segura, elocuente, inspiradora y ocurrente; con sus gafas rectangulares y un traje azul brillante irradiaba energía. Habló durante treinta minutos y resumió una extensa trayectoria: su ingreso en la Iglesia, algunas de sus experiencias no del todo agradables (como el intento de la Iglesia de disuadirla de que tomase la medicación para la epilepsia), la visión de la mecánica de lavado de cerebro empleada por la Iglesia («Es un lento tren de control mental», según sus palabras) y descripciones de las tendencias teológicas de la Iglesia transmitidas mediante costosas clases («Mantener la Cienciología en funcionamiento es una máxima en todos los cursos»). En la parte final de su exposición describió su espeluznante huida («[la Cienciología] me persiguió por todo el país») y subrayó la mayor ironía de la Iglesia («venden libertad

pero te esclavizan»).

Ella también reconoció explícitamente el papel de Anonymous: «Hoy todo el mundo puede permitirse ese lujo [de hacerlo público] gracias a: (A) Internet; (B) los críticos incluso antes de Anonymous; y (C) Anonymous. ¿Verdad? Que fue algo que cambió absolutamente las reglas del juego. Para siempre. Así fue y todos lo sabemos.» Tory destacó la valentía de una generación anterior de críticos, un puñado de ellos presente en la sala, que decidieron salir a la luz cuando el número de desertores era muy bajo y la Cienciología tenía el poder de destrozar sus vidas colocándolos agresivamente en el punto de mira y con total impunidad. «Anonymous no estaría aquí si no fuese por los críticos que alzaron sus voces antes que ellos», añadió.

Su siguiente afirmación reverberó a cámara lenta a través de la sala y nos conmovió a todos: «No hay manera de que la Cienciología pueda derrotarnos más. Se acabó.» Es probable que a los ex cienciólogos allí presentes estas palabras les alcanzasen con una combinación de alivio y alegría. Los Anons, algunos de los cuales habían estrechado su relación con ex cienciólogos, probablemente se sintieron bañados por el orgullo de haber conseguido un logro político. No hay nada, *nada,* comparable al sabor dulce de la victoria política y Chanology había desafiado a una organización que parecía omnipotente, inmune a la crítica y por encima de la ley.

Más notable aun es que lo que comenzó como una política estrechamente configurada y lanzada contra un único enemigo, excedió ese marco para abarcar a una empresa política más consistente, diversa y absolutamente global, una hoguera que ardió y brilló el tiempo suficiente para extenderse a través del planeta, convirtiéndose en Anonymous en todas partes. Examinemos ahora los hechos improbables que impulsaron el sorprendente ascenso de Anonymous.

Capítulo 3

Las armas de los geek

WikiLeaks: el regalo permanente

Era el 20 de julio y asistía a una conferencia llamada Hackers on Planet Earth ("Hackers en el planeta Tierra"), también conocida como HOPE, que se celebraba cada dos años en el histórico (y, por su parecido con el hotel de *El resplandor*, también aterrador) hotel Pennsylvania de Nueva York. Una vez acabada mi intervención, me sentía preparada para absorber aquel ambiente tan extraordinario y políticamente cargado de dramatismo, intriga y suspense. Pero el ambiente cargado que reinaba en HOPE no era a consecuencia de Anonymous. En aquel momento, si bien ya se podía describir a Anonymous como políticamente extravagante, en términos geopolíticos el grupo tenía una escasa importancia real. Los activistas de Anonymous habían comenzado a participar en otros escenarios (como la Revolución verde iraní), pero seguían centrados sobre todo en Chanology, exponiendo con tenacidad los abusos cometidos por la Iglesia de la Cienciología y manifestando sus protestas todos los meses en ciudades de Norteamérica, Australia, Europa y algunos otros lugares. Un número considerable de trols seguía reclamando el nombre de Anonymous, pero esta corriente de "cabronadas ultracoordinadas" se encontraba en claro declive.

No, la intriga que saturaba la conferencia se debía a la presencia de otro jugador en el terreno de juego: WikiLeaks, la sensación de las denuncias. Más concretamente, el interés se centraba en torno al nuevo

tesoro de documentos y material filmado que había filtrado un joven soldado del ejército llamado Chelsea Manning (antes Bradley Manning) para servirlo al mundo entero a través de WikiLeaks. Fundado en 2006, el concepto impulsor detrás de WikiLeaks había sido simple: proporcionar una casa segura y un catalizador de información para las filtraciones. WikiLeaks llevaba años desarrollando esta actividad, poniendo en circulación innumerables filtraciones, pero no había conseguido atraer la atención de importantes instituciones mediáticas como el *New York Times*. Esta falta de atención no se debía a que las filtraciones carecieran de valor. De hecho, algunas de ellas —como la noticia de que la multinacional Trafigura había realizado vertidos tóxicos ilegales frente a Costa de Marfil— eran alarmantes y estaban alarmantemente ausentes de los principales medios de comunicación. Tampoco se debía a que no lo hubiesen intentado, al menos no sólo para eso. El gobierno británico había impedido que el periódico izquierdista *The Guardian* cubriese la historia de Trafigura. Como señalaron los editores en aquel momento, «a *The Guardian* también se le prohíbe que cuente a sus lectores por qué se impide —por primera vez en la historia— informar al Parlamento. Obstáculos jurídicos, que no se pueden identificar, incluyen procedimientos, que no se pueden mencionar, en nombre de un cliente que debe mantenerse en secreto.»[47]

Fue en abril de 2010 cuando WikiLeaks cambió de manera radical su estrategia de comunicación. Nada, al publicar un vídeo con las imágenes de un ataque aéreo sobre Bagdad bajo el título “Asesinato colateral”, fue dejado al azar; WikiLeaks envolvió el ya de por si impactante material para que produjera un impacto adicional. Editaron el vídeo para que tuviese el máximo efecto y añadieron al principio un comentario editorial simple pero contundente. Julian Assange, el hacker australiano fundador de WikiLeaks, era conocido entonces en los medios de comunicación como un “misterioso agente internacional”. Ahora rompía con su anterior reticencia a ser el centro de atención. Coincidiendo con la publicación del vídeo, Assange convocó una rueda de prensa en Washington, D.C., seguida de una gira mediática de altos vuelos.

La respuesta periodística y pública fue explosiva. Christian Christensen, el experto en medios de comunicación, afirma que el vídeo es «uno de los resultados más conocidos y más ampliamente reconocidos del proyecto WikiLeaks en curso», porque aporta una «evidencia visual del

flagrante abuso del poder estatal y militar».[48] Las imágenes en blanco y negro están captadas desde la perspectiva de un soldado a bordo de un helicóptero de ataque *Apache* mientras acribilla a balazos a un grupo de civiles en un suburbio de Bagdad. El vídeo, grabado en 2007, suscitó muchas preguntas. ¿Por qué no habíamos visto antes estas imágenes? Dos de los hombres asesinados durante el ataque eran periodistas que trabajaban para la agencia de noticias Reuters, que en los años transcurridos desde el ataque había estado tratando de conseguir la filmación a través de una solicitud amparada por la Ley de Libertad de Información. Sospechaban que había gato encerrado y sus sospechas no eran infundadas. El vídeo era un embarazoso recordatorio de cómo los principales medios de comunicación habían fracasado en su misión de informar al público, volviéndole la espalda al estilo de reportajes de guerra directos y terribles practicados en los últimos años de la guerra de Vietnam.

Sin embargo, lo que realmente ponía los pelos de punta, más que cualquier otra cosa, era el tono banal de los pilotos durante las conversaciones mantenidas con su mando sobre si debían atacar ese objetivo: transmitían una tranquilidad que rozaba la psicosis. Un miembro de la tripulación se echa a reír al descubrir que una de las víctimas es una niña pequeña. «Bueno, la culpa es de ellos por traer a sus hijos a la guerra», comenta con indiferencia.

Como todos sabemos ahora, Chelsea Manning decidió filtrar el vídeo, acompañado de otros documentos sensibles, y un hacker llamado Adrian Lamo la delató a las autoridades. El 22 de mayo de 2010, Manning le confesó a Lamo durante una conversación por chat que había entregado a WikiLeaks las imágenes utilizadas para crear “Asesinato colateral”. Al principio de la conversación, Lamo se gana la confianza de Manning haciéndose pasar por otra persona:

> Soy periodista y pastor. Puedes escoger cualquiera de los dos y tratar este asunto como una confesión o como una entrevista (que nunca será publicada) y disfrutar de una pizca de protección legal.[49]

Manning se desahogó entonces con una persona a la que no conocía de nada y cuyas afirmaciones de ser periodista y pastor eran, en el mejor de los casos, poco fiables.[50] Lamo entregó el registro al FBI y a la revista *Wired*.

El FBI arrestó a Manning, y la obligó a confesar finalmente que había proporcionado a WikiLeaks no solo las imágenes de vídeo que se veían en "Asesinato colateral", sino también los cables diplomáticos que WikiLeaks haría públicos a lo largo de los dos años siguientes. Manning fue condenada por un juez militar a treinta y cinco años de prisión y actualmente se encuentra recluida en Fort Leavenworth, después de haber sufrido un año de confinamiento en solitario previo a su condena.[51]

En la conferencia de HOPE en 2010 la tensión se palpaba en el ambiente. Se rumoreaba que Julian Assange pronunciaría el discurso de apertura. En un cambio de última hora, no fue Assange quien subió al estrado sino el hacker estadounidense Jacob Appelbaum. Su fascinante intervención le reveló efectivamente, delante de todos los presentes en la sala (incluidos los inevitables agentes federales), como un afiliado a la organización sitiada. Fue un gesto audaz, teniendo en cuenta las tácticas de silenciamiento, acusación e intimidación dirigidas contra la organización por las autoridades de Estados Unidos. Su disertación contextualizó históricamente a WikiLeaks dentro de lo que hoy se suele denominar "el quinto poder": los hackers, filtradores, periodistas independientes y blogueros que cumplen el papel crítico que alguna vez recayó en "el cuarto poder", los medios de comunicación dominantes. O, en palabras de Appelbaum, «cuando amordazan a los medios de comunicación, nosotros nos negamos a ser amordazados. Nos negamos a ser silenciados», declaración que fue recibida con una ensordecedora ovación. (El ejemplo más flagrante del silencio de los medios de comunicación en la pasada década se produjo cuando el *New York Times* se negó, a petición del gobierno, a publicar una historia sobre las escuchas ilegales, sin contar con una orden judicial, llevadas a cabo por la NSA. El *Times* finalmente publicó la historia solo porque el autor, James Risen, estaba a punto de robarle la primicia al periódico publicando un libro sobre esa delicada cuestión. El artículo que las autoridades intentaron ocultar con tanto ahínco acabó obteniendo un Premio Pulitzer.)

Si bien WikiLeaks, "Asesinato colateral" y Manning se habían hecho un lugar importante en las charlas entre hackers con conciencia política y defensores de la transparencia, una cuarta figura dominaba la mayoría de las conversaciones en HOPE: Lamo, el hacker traidor. Estaba en boca de todo el mundo por una razón muy sencilla: era, igual que ellos, un hacker y,

para colmo, estaba presente en la conferencia. La gente estaba absolutamente indignada. Durante su disertación sobre WikiLeaks, Appelbaum prometió no pronunciar ni una sola palabra sobre Lamo. Mientras lo decía se desabrochó la camisa para mostrar una camiseta en la que se leía «Basta de chivatazos». La gente se volvió loca. La sala se llenó de folletos con la cara de Lamo. Lamo era «BUSCADO// Vivo o Muerto // por ser un puto chivato cabrón».

Mientras contemplaba el folleto, un hacker amigo se acercó a saludarme. Moviendo la cabeza con disgusto por el tema de Lamo, mi amigo me explicó que Assange era «lo realmente importante», un elogio extraordinario viniendo de un compañero hacker. Le había conocido en la década de 1990 cuando el hackeo underground estaba en pleno auge y se manifestaba libremente, antes de que se tomaran medidas contundentes contra ellos a finales de esa década. Esta clase de hacker ignoraba rutinariamente la ley en sus exploraciones de redes privadas y sistemas informáticos, no por maldad o por obtener un beneficio económico sino por su curiosidad insaciable: un deseo de saber cómo funcionan las cosas. Aunque la transgresión en sí ofrecía una forma de placer, en aquella época solo un reducido grupo de hackers estaba explícitamente orientado a la militancia política. Julian Assange era uno de ellos. Era un hacker plenamente convencido que incluso redactaba manifiestos éticos para explicar sus acciones. Assange formaba parte de un reducido grupo de "subversivos internacionales" que se atenían a un credo: «No dañar los sistemas informáticos a los que accedas (incluye aplastarlos); no cambiar la información que haya en esos sistemas (excepto alterar los registros para borrar tus huellas); y compartir información.»[52]

Cuando terminábamos nuestra conversación sobre Assange, mi amigo y yo escuchamos una noticia emocionante. El principal organizador de HOPE, Eric Corley —más conocido por su famoso handle de hacker "Emmanuel Goldstein"— había anunciado un panel improvisado sobre chivatos y chivatazos presentando nada menos que al propio Lamo.

Estaba previsto que Lamo se sentara al lado de algunos de los más famosos phreaks telefónicos y hackers underground de todos los tiempos: Bernie S., Mark Abene (también conocido como Phiber Optik) y Kevin Mitnick. Un par de ellos habían estado en la cárcel por chivatazos. Ellos mismos, en sus propios juicios y penas, se habían negado a "cooperar" y lo

habían pagado caro, con una ampliación de sus condenas por mantener la boca cerrada y no delatar a sus compañeros.

En todos los años que llevo asistiendo a conferencias de hackers, este panel sigue siendo el más extraordinario que he visto jamás. Imaginad a 2.600 hackers sentados delante de un único traidor despreciado por todos, mientras él les mira desde el estrado y trata de justificar sus acciones.

CONSEJO HACKER SOBRE CHIVATAZOS CON EL HACKER SOPLÓN MÁS TRISTEMENTE FAMOSO DE TODOS LOS TIEMPOS

Los hackers abrieron el panel relatando historias fascinantes sobre sus hazañas, detenciones y traiciones a manos de compañeros en los que confiaban. El primero en dirigir la palabra a los presentes fue Goldstein, quien subrayó una obviedad que yo vería en acción poco después con Anonymous. Cuando aparecen los federales o la policía (habitualmente al amanecer y golpeando la puerta violentamente al tiempo que apuntan con sus pistolas), recordó Goldstein al público, «la gente siente pánico... y las autoridades lo aprovechan. Las autoridades viven para esta clase de situaciones con el fin de obtener la máxima información posible, consiguen que todos nosotros delatemos a otras personas.»

Cuando Lamo subió al estrado y se dirigió lentamente a su asiento, bueno... las bolsas debajo de sus ojos eran de un marrón intenso y cuando parpadeaba lo hacía a cámara lenta y con gran dificultad, como si tuviera que forzar los párpados hacia abajo cada vez. No es que pareciera nervioso, parecía estar muy colocado; es muy posible que, además de agotado, estuviera medicado. Elogiado en otro tiempo como un hacker de sombrero negro, escuchar a Lamo justificar sus acciones resultaba fascinante. Se sintió "obligado", explicó, a entregar los registros en interés de la defensa nacional. Bernie S., deseoso de conocer más detalles, le interrumpió respetuosamente: «¿En qué sentido pensaste que se estaba poniendo a la gente en peligro?» Lamo dio una respuesta farragosa: «El Departamento de Estado está implicado en una serie de operaciones de inteligencia en todo el mundo, hmmm…, se supone que no debe hacerlo, pero está protegiendo los intereses de los americanos.» Estas palabras provocaron el inmediato abucheo de la multitud y un miembro del público gritó, «¡son las

actividades del Departamento de Defensa las que ponen en peligro a la gente!»

Goldstein percibió que el público podía convertirse en una turba dispuesta al linchamiento, afilando sus cuchillos y encendiendo las antorchas, preparada para echar a Lamo de la ciudad. Tranquilizó a los presentes recordándoles que «podréis dar vuestra opinión», pero no antes de que Phiber Optik soltara, entre risas, «repartiremos dardos y arcos y flechas, no os preocupéis». Esa intervención humorística liberó algo de presión, pero la atmósfera de tensión se mantuvo hasta el final. Una y otra vez los intentos de Lamo de racionalizar sus acciones se topaban con abucheos airados. Después de que Lamo defendiese al gobierno y describiera sus relaciones con sus agentes como «una tarea sorprendentemente agradable», ni siquiera Goldstein fue capaz de contenerse; interrumpió a Lamo antes del turno de preguntas para preguntarle cómo se sentía ante la posibilidad de que Manning pudiera pasarse el resto de su vida en prisión (alguien de la multitud también gritó «¡Tortura!»). Sin alterarse, Lamo respondió lentamente: «Nosotros no le hacemos eso a nuestros ciudadanos.» Algunos de los abucheos y pitidos más estruendosos del día recorrieron la sala y alguien gritó: «¡Guantánamo!» No importaba lo que Lamo dijera, era evidente que se estaba enterrando en un agujero cada vez más profundo y también era obvio que prácticamente todo el auditorio estaba dispuesto a echarle encima la última palada de tierra.

En aquel momento, a pesar de lo apasionante que era el grupo que ocupaba el estrado, no alcanzaba a ver la relevancia que aquello podía tener para mi proyecto sobre Anonymous. WikiLeaks y Anonymous, en aquellos días, habitaban en planetas diferentes (aun cuando estuvieran, desde luego, en la misma extravagante galaxia con sus respectivas luchas contra la censura y la Cienciología).[53] Sin embargo, un año después de la conferencia, el 4 de julio de 2011, tuve mi primer chat privado en IRC con el soplón más famoso de Anonymous: Héctor Monsegur, a quien previamente solo se le conocía como “Sabu”. Para entonces ya había sido arrestado y trabajaba en secreto para el FBI, aunque en aquella época lo ignorásemos yo y mucha otra gente (a pesar de una lista interminable de pistas que hoy resultan obvias). El carisma de Monsegur —y su habilidad en tácticas de guerra psicológica, como traspasar a otros las sospechas y acusarles de soplones— ocultaba muchos de los indicios que dejaba caer en

texto simple unos meses después de su arresto encubierto: «Limitáos a vosotros mismos», escribió en reddit. «Si estás en un equipo, mantén las operaciones de seguridad las 24h del día. Los amigos intentarán eliminaros si tienen que hacerlo».[54] Estas advertencias repetían una lección que Manning había aprendido de primera mano un año antes.

Pero el problema recíproco relacionado con los soplones es el menor de los contactos emergentes entre WikiLeaks y Anonymous. Podemos rastrear una relación más directa examinando la trayectoria de la plataforma AnonOps.

DDOSEANDO CON UNA TIRADA DE DADOS AL AZAR

AnonOps apareció en 2010, apenas unos meses después de que acabase HOPE. Comenzó como un nuevo nodo de Anonymous y con el tiempo se convirtió en una auténtica red de IRC. La red tomaría el mundo por asalto gracias a sus experimentos —y digo, literalmente, experimentos, ya que el grupo nunca reflexionó en serio hasta mucho más tarde— con un montón de tácticas políticas de acción directa. Muchas de estas tácticas eran directamente ilegales, de modo que era solo cuestión de tiempo que llamasen la atención del FBI.

Aunque la historia de AnonOps se cruzaría con la de WikiLeaks en diciembre de 2010, desde la perspectiva de la mecánica organizativa ambas entidades no podían ser más distintas. WikiLeaks se desarrolló como un trabajo vital cuidadosamente diseñado. Assange, como fundador y portavoz, controlaba —demasiado de cerca, dirían muchos— la mayoría de los aspectos, y su personalidad e identidad se fusionaron inevitablemente con el nombre de WikiLeaks. Que su reputación personal fuera mancillada perjudicó al conjunto de la organización. Por su parte, la constitución de AnonOps fue un hecho fortuito, como el Proyecto Chanology antes que él: nacidos de la convergencia contingente de oportunidad y atención de los medios de comunicación, cada elemento contribuyó a su meteórico ascenso y a su rápido éxito, recordando, una vez más, cómo los embaucadores como Anonymous están perfectamente preparados para explotar los accidentes que les sirven en bandeja y, en ocasiones, se benefician de actuar por puro capricho.

Eran los últimos días de agosto de 2010, alrededor de dos años y medio después de que los hackers adoptasen por primera vez el nombre Anonymous y se aventurasen en el mundo del activismo. Para entonces, Chanology había organizado protestas callejeras, había forjado estrechas alianzas y amistades con ex cienciólogos, se había implicado en la infructuosa Revolución verde iraní, y se había diversificado hacia otras áreas del activismo en Internet. En febrero de 2010, después de que el Ministro de Telecomunicaciones de Australia propusiera una reglamentación para filtrar los contenidos pornográficos en Internet, algunos Anons emprendieron la Operación Titstorm (literalmente, "tormenta de tetas") y consiguieron saturar los servidores del gobierno con una avalancha de solicitudes de tráfico. Esta operación, anunciada como parte de la Operación Freedom Movement, fue un presagio de lo que aguardaba en el horizonte.

Un grupo de Anons relanzó la Operación Freedom Movement, renovando el Internet Freedom Movement (IFM), el 5 de julio, once días antes de HOPE.[55] Las personas que participaban en el IFM, junto con el conjunto del mundo geek, se habían propuesto protestar contra el Acuerdo Comercial Antifalsificación (ACTA). El ACTA buscaba, entre otras consideraciones, introducir amplias regulaciones destinadas a criminalizar la vulneración de los derechos de autor y animar a los proveedores de servicios de Internet a retratar, rastrear y controlar a sus usuarios. La oposición a estas medidas fue feroz y prácticamente todos los grupos implicados en la política de acceso a la red —Electronic Frontier Foundation, Free Software Foundation, Public Knowledge, La Quadrature du Net— criticaron el secretismo con el que se negociaba el tratado y se opusieron categóricamente a su ratificación.

La metodología propuesta por el IFM consistía en presionar a los políticos y sensibilizar a la opinión pública utilizando materiales de propaganda y sitios web. Como parte de estas iniciativas, los activistas crearon una sala de chat específica llamada "#antiactaplanning" en el servidor de IRC OccultusTerra. A finales de agosto de 2010, un activista de Anonymus bajo el apodo de "golum" (no era su seudónimo habitual) accedió a la sala de chat y declaró audazmente su intención de hacer que las cosas avanzaran mediante ataques DDoS contra el sitio web de la Oficina del Representante de Comercio de Estados Unidos (USTR), ustr.gov, a las

21 h del 19 de septiembre de 2010. La oficina del USTR era una elección natural si se considera que el ACTA era un acuerdo comercial liderado por Estados Unidos y el USTR tenía la potestad de sancionar a aquellos países que violasen los tratados comerciales.

Pero muchos de los que participaban en la sala de chat tenían dudas sobre esta acción: en primer lugar, Chanology ya había establecido un precedente político al rechazarse el uso de tácticas ilegales como el DDoS. Y, en segundo lugar, nadie podía entender por qué se había elegido esa fecha en particular. A muchos les pareció algo absolutamente arbitrario y (en gran parte) lo era; la única conexión era que el 19 de septiembre se celebra el Día Internacional de Hablar como un Pirata. Golum se encontró con una firme oposición, al menos por parte de aquellos que prestaban atención a las pantallas (todos los seudónimos han sido cambiados):

<matty>: ¿por qué antes de que se haya firmado?
<golum>: Porque es un domingo y a todo el mundo le gustan los domingos
<matty>: repito ... ¿por qué antes de que se haya firmado?
<golum>: Y porque lancé un dado
<golum>: Y dice el 19 [...]
<golum>: Mi predicción es que para el 19 de septiembre la gente tomará más conciencia.
<golum>: Confía en mí. El 19 de septiembre.
<fatalbert>: confía en mí en un día que lanzas los dados al azar

Aunque todos en el canal atacaron salvajemente la propuesta de golum, él permaneció impertérrito:

<golum>: Como queráis, escuchad. He escuchado todos los argumentos para NO ddosear. Pero la verdad es que necesitamos hacer que despierten. [...]
<golum>: Entiendo que ddosear podría perjudicar potencialmente nuestra causa.
<golum>: Pero creo que merece la pena correr el riesgo.
<fatalbert>: bueno, por mi parte no estoy de acuerdo y por lo tanto no ayudaré a ddosear el sitio
<golum>: Necesitamos atención
<+void>: OMG ES ANONYMOUS, LO ÚNICO QUE HACEN ES DDOSEAR, OMGOMGOMOGMOMG HAGAMOS QUE ACTA SE APRUEBE EN POSITIVO
<golum>: No.
<golum>: matty, ¿cómo ha ido el contacto con los políticos?

<BamBam>: Sí yo siempre he odiado el ddos
<golum>: Mirad. He escuchado los argumentos y solo quiero decir que deberíamos hacer esto.
<golum>: Ahora NO estamos ddoseando. Esto se hará dentro de 20 días.
<golum>: 20 días es mucho tiempo.

Unos cuantos Anons, expresando los riegos jurídicos, destacaron la diferencia entre atacar al gobierno de Estados Unidos y hacerlo a otros objetivos, y dieron por terminada la conversación. (Cabe señalar también que la evaluación del riesgo de ser arrestados era correcta —más de veintisiete personas han sido procesadas desde entonces por la subsiguiente avalancha de acciones relacionadas con el DDoS— y en los Estados Unidos aún puedes meterte en serios problemas por atacar en la red a cualquier persona famosa.):

<matty>: Este no es justin bieber, es el gobierno de los Estados Unidos [joder] [...]
<golum>: Todo el mundo, por favor, escuchadme cuando hablo
<AnonLaw>: Me partiré de risa cuando te metan en la cárcel
<matty>: Yo no estoy aquí por el puto lulz [...]
<golum>: Es oficial. Comienzo a prepararlo.

Si se están preguntando qué significa “oficial” en Anonymous... bueno, sí, alguna cosa puede ser considerada “oficial” si alguien la declara como tal y, fundamentalmente, si un número suficiente de personas también la respalda. Pero en aquel momento se carecía de apoyo para las tácticas militantes de acción directa en este canal de IRC. Aunque alguien había iniciado un canal de IRC llamado “#ddos” con el fin de analizar el posible uso de esta táctica, el aspecto anárquico del chat de IRC de Anonymous solo llega hasta donde topa contra normas y disposiciones:

<Lola>: ¿Qué pasó con #DDoS?
<Fred>: Considéralo off topic por favor.
<Fred>: Esto es estrictamente una planificación para ACTA.
<Fred>: No para una charla frívola
<Lola>: #ddos era un canal de planificación para ACTA.
<Lola>: Quiero saber qué pasó con él.
<Fred>: Las preguntas sobre #ddos están fuera de tema.
<Fred>: Es para planificar.

<Yagermister>: #DDoS es MALO

Al día siguiente Lola volvió a aparecer, en esta ocasión para hablar sobre las botnets (redes de ordenadores controlados a distancia que pueden utilizarse para reforzar un ataque DDoS):

<Lola>: ¿Tenéis una botnet?
<Lola>: sin una no podéis hacer mucho
<Lola>: podéis conseguir unos 10 $ por 100 en estos días
<Lola>: de algunos foros skiddie

A Lola le advirtieron, nuevamente, que dejase de «hablar de actividades ilegales».

Tal vez éste sea un momento oportuno para hablar de las botnets con mayor detalle, sobre todo desde que se volvieron cada vez más importantes para las operaciones DDoS llevadas a cabo por Anonymus y que analizaremos más adelante. En todo este asunto hay una faceta que recuerda al robo de ganado que se practicaba en el Lejano Oeste. Una botnet es básicamente una serie de ordenadores conectados a Internet que permiten contar así con una única entidad extra que procesa conexiones eléctricas o de red para la ejecución de diversas tareas, incluidas (pero no limitadas a) el DDoS y el bombardeo con correo basura. Una botnet es una herramienta muy poderosa que implica (tal como lo hace) a ordenadores conectados en distintas partes del mundo y que son capaces de distribuir tareas. Los participantes cuyos ordenadores están conectados habitualmente para participar en una botnet ignoran que sus ordenadores son utilizados para este propósito. ¿Te has preguntado alguna vez por qué tu ordenador funciona tan lento o de un modo tan extraño? Bueno, quizás hayas participado involuntariamente en un DDoS.

A menudo un ordenador se convierte en miembro de una botnet al ser infectado con malware (software malicioso). Esto puede suceder mediante una serie de métodos diferentes: ese divertido vídeo sobre gatos que has descargado, el enlace malicioso en un correo electrónico de tu tía, un ataque de phishing (suplantación de identidad) del que no tenías idea, o un virus oculto en algún software que descargaste de Internet. Una vez ha sido infectado, el ordenador ejecuta un pequeño programa, habitualmente oculto

en la tabla de procesos de modo que no resulte fácil detectarlo, que arbitra su participación en la botnet.

Si bien existen muchas maneras diferentes de funcionamiento de una botnet, un método clásico incluye su conexión a un canal y servidor de IRC preconfigurados. Una vez hecha esta conexión, el ordenador esperará pacientemente —sin que sus dueños lo sepan— hasta recibir las órdenes del pastor de la botnet (¡yupi!). El pastor es el individuo capaz de dirigir los ordenadores que integran la botnet. Habitualmente se trata de la persona que primero ha infectado los ordenadores. En general, está esperando en el canal de IRC designado, con una sonrisa de oreja a oreja mientras aumenta el número de ordenadores infectados que se incorporan al canal, como zombies que aguardan una orden. A esto se lo conoce como canal de mando y control (C&C). Un escenario típico podría ser un pastor saltando adelante y atrás entre canales de chat regulares y el canal C&C oculto mientras se vuelve cada vez más poderoso.

Una botnet típica podría presumir de tener alrededor de veinte mil ordenadores, pero las botnets más grandes han sido rastreadas hasta contabilizar treinta millones de aparatos infectados. (Aunque la mayoría de las botnets tienen mala fama —y con razón—, algunas de ellas son voluntarias y participativas. La más famosa probablemente sea SETI@home, la cadena de tres millones de ordenadores que buscan vida alienígena en el espacio exterior.) Los ordenadores se desplazan por este canal C&C hasta que el pastor de la botnet les da una orden —habitualmente verificada— para que lleven a cabo alguna tarea. Por ejemplo, el pastor de la botnet podría decir simplemente, «ddos 172.16.44.1» y entonces todos los programas robot conectados comenzarán a atacar esa dirección específica de IP.[56]

Otra tarea común para las botnets consiste en enviar enormes cantidades de correos electrónicos no deseados. El correo basura es interceptado a menudo por un algoritmo que determina su naturaleza no deseada y bloquea la dirección de envío, pero cuando decenas de miles de máquinas diferentes con direcciones diferentes están enviando el correo basura, es mucho más complicado de rastrear y detener. Con frecuencia los pastores de las botnet unen su red no para alcanzar sus propios objetivos, sino para vender los servicios de sus programas a un emisor de correo basura.

Tener la capacidad de controlar decenas de miles de ordenadores desde una ubicación central es una sensación poderosa. Mediante la simple acción de emitir órdenes se puede conseguir que miles de ordenadores hagan algo para ti, y cuanto mayor sea el número de ordenadores que participan en la red, más potentes serán estas órdenes. En el mundo de las botnets existe una lucha permanente por quién tiene más programas robot, el mayor ancho de banda y las máquinas mejor infectadas (los ordenadores de universidades, corporaciones y gobiernos tienden a estar en el mejor ancho de banda).

Esta competencia es tan feroz que, a menudo, los pastores de las botnets intentarán tomar el control de otras botnets. Al otro lado de la valla, los organismos encargados de hacer cumplir la ley y las organizaciones individuales que luchan contra el correo basura también se esfuerzan por hacerse con el control de las botnets para neutralizarlas. No se trata de una tarea trivial. Primero uno debe identificar el C&C. Si puedes determinar de dónde reciben sus órdenes los programas robot, puedes unirte al canal de IRC, enmascarado como una máquina comprometida, y esperar a recibir un comando del pastor de la botnet. Si el pastor envía una autentificación junto con el comando, puedes obtener la contraseña necesaria para emitir órdenes a toda la botnet.[57]

Pero, como señalaba Lola, también se puede acceder a todo ese poder y diversión mediante una “tarifa de suscripción” realmente barata. La gente en el servidor de IRC no estaba nada satisfecha con toda esta conversación sobre el submundo de las botnets y los DDoS. Los operadores del IRC eliminaron del servidor al contingente pro DDoS. Se marcharon, inasequibles al desaliento, para convertirse en nómadas de Anonymous.

Resulta tal vez irónico que golum, según me explicó uno de los participantes, «fuera una figura central en el movimiento IFM, cuando no LA figura central». Es posible que golum haya encabezado la iniciativa, pero su influencia fue desapareciendo paulatinamente cuando insistió en aplicar la clase de tácticas digitales que eran firmemente rechazadas por la mayoría de Anons al frente de Chanology. En efecto, esta mayoría consiguió «cambiar la dirección de la operación» con el fin de mantenerla dentro de un marco absolutamente legal. Aquellos que querían utilizar técnicas de acción directa se encontraron cada vez más marginados. Pero mientras que la visión de echar los dados al azar preconizada por golum puede haber parecido nada más que, bueno, azarosa, golum era de hecho un

hábil organizador con una aguda percepción de la dinámica que caracterizaba a los medios de comunicación. Yo le había visto en acción en numerosas ocasiones y era uno de los mejores propagandistas y organizadores con los que contaba Anonymous. Golum se marchó del movimiento IFM para formar una nueva facción orientada hacia la acción directa y se llevó con él a algunos Anons. Uno de los participantes en esta nueva empresa militante, que llegaría a ser conocida como AnonOps, describió a golum como un tío con «una antena muy, muy buena para las relaciones públicas y la propaganda y comprendía (en aquel momento) el inmenso impacto psicológico que causaba declarar que un sitio web desaparecería, y luego hacerlo».

Golum se marchó con sus tácticas, y sus partidarios, a otra parte. Curiosamente, teniendo en cuenta su anuncio del día de la tirada de dados al azar, había creado de hecho un sitio web con un calendario para la protesta contra el ACTA que difería del anunciado previamente en el canal de IRC. El sitio designaba el crescendo de actividades previstas para el 5 de noviembre, la jornada de protestas convocadas en todo el mundo y conocida como Día de Guy Fawkes.

Golum había concebido diferentes grupos divididos por salas de chat (#bump, #newor, #op), cada uno con funciones y responsabilidades específicas.

La confusión se cernía sobre la fecha de inicio de la campaña DDoS, pero al final, gracias a la iniciativa de algunos actores desconocidos, habría de caer a mediados de septiembre, tal como golum había anticipado. Una contundente y espectacular avalancha de ataques DDoS atrajo a más de setecientas personas a la sala de chat del grupo disidente y se prolongó durante más de dos meses. Finalmente no colocaron en el punto de mira a la Oficina del Representante de Comercio de Estados Unidos. En cambio, en una acción en defensa del intercambio de archivos, lanzaron un tremendo ataque DDoS contra una serie de asociaciones defensoras de los derechos de autor, como la Asociación Cinematográfica de Estados Unidos (MPAA) y la Asociación de la Industria Discográfica de Estados Unidos (RIAA). La atención que les dedicaron los medios de comunicación fue considerable y el nuevo grupo se quedó enganchado. Exhibiendo el logotipo del barco de The Pirate Bay —adoptado también por Anons como símbolo de sus campañas– la BBC informó: «Los activistas de la piratería han lanzado

ataques coordinados contra sitios web propiedad de las industrias musical y cinematográfica.»[58] Anonymous incluía todos los reportajes y noticias escritos sobre la “Operación Venganza” —como la llamaba el grupo— en tieve.tk, que también se convirtió en el centro de consulta de información mientras Anonymous emigraba de servidor IRC en servidor IRC antes de establecer uno propio a finales de octubre.

A la luz de mis experiencias con Anonymous, puedo afirmar con toda seguridad que si el grupo disidente de golum simplemente hubiera reunido algunas tropas alrededor de un eslógan como “el ACTA apesta”, las oleadas de apoyo sin precedentes jamás se hubieran materializado. Afortunadamente, el espíritu de Puck aportó un delicioso accidente a este incipiente equipo de Anonymous. Fue como si Eshu, el embaucador de las encrucijadas en la religión yorubá, apareciera para instarles a tomar una decisión. Como veremos, su elección permitió que la semilla germinase y diese lugar a una de las mayores sensaciones políticas de Internet.

«A veces debemos hacer un esfuerzo adicional y atacar el sitio»

La información que cambió las reglas del juego apareció en un artículo sobre tecnología publicado por un medio de comunicación indio el 5 de septiembre de 2010. A los periodistas occidentales les llevó toda una semana hacerse eco de la noticia y, a partir de ese momento, comenzó a circular por la prensa técnica de Internet. La historia cita al Director general de Aiplex, una empresa india de software supuestamente contratada por las corporaciones para lanzar ataques DDoS contra sitios de intercambio de archivos como The Pirate Bay:

> El problema está en los sitios para descargar archivos torrent, que habitualmente no cumplen [cuando reciben una solicitud legal por escrito para eliminar una película]. En esos casos, inundamos el sitio web con montones de solicitudes, lo que provoca un error en la base de datos, causando la denegación de servicio ya que cada servidor tiene una capacidad de ancho de banda fijo. A veces tenemos que hacer un esfuerzo adicional y atacar el sitio y destruir los datos para impedir que la película siga circulando por la red.[59]

Irónicamente, teniendo en cuenta el objetivo, esa confesión proporcionaba la prueba de una práctica contemporánea análoga a la actividad de los corsarios en el pasado. Hasta que los declararon fuera de la ley en 1856, las potencias europeas contrataban habitualmente a piratas para que operasen como sus agentes en alta mar, con la ventaja añadida de que podían ocultar su propia implicación en cualquier asunto desagradable que requiriese la intervención de los bucaneros. No era la primera vez que aparecían pruebas de que las industrias de los derechos de autor contrataban técnicos para que llevasen a cabo su trabajo sucio (e ilegal). En 2005, la MPAA contrató a un hacker para que se infiltrase en los servidores de TorrentSpy, un motor de búsqueda de material de intercambio de archivos, y buscase información confidencial que les proporcionara pruebas de que estaban violando la ley. En el curso de una entrevista exclusiva con Wired.com, este hacker explicó cómo la MPAA intentó seducirle con dinero en metálico y artículos de lujo: «Necesitamos a alguien como usted. Le proporcionaríamos un agradable trabajo remunerado, una casa, un coche, cualquier cosa que necesitara... si salva a Hollywood para nosotros, podrá hacerse rico y poderoso.»[60]

En el caso de Aiplex, era la primera vez que ese reconocimiento era tan franco y directo.

Como cabía esperar, la reacción de Anonymous y de muchos otros grupos geek de Internet fue rápida y mordaz. Durante más de una década, el extraño híbrido industria/lobbys/asociaciones de representantes de derechos de autor invirtieron millones de dólares para perseguir agresivamente y demandar a las personas que compartían archivos y a los hackers que dirigían sitios P2P, como The Pirate Bay, que coordinan el acceso a tesoros ocultos de material sujeto a derechos de autor. Ahora había segmentos de la industria de los derechos de autor dispuestos a hacer un "esfuerzo adicional" contratando a hackers para que participasen en tácticas ilegales propias con el propósito de reprimir el intercambio ilegal de archivos.

Los geeks criticaron los métodos técnicos empleados por Aiplex (es muy habitual que los geeks aprovechen todas las oportunidades para debatir los méritos de cualquier avance tecnológico). Se burlaron de la terrible y estúpida confesión criminal como estrategia de comunicaciones de Aiplex. En TorrentFreak, un popular sitio web dedicado a dar noticias sobre el intercambio de archivos, un comentarista señaló: «Aiplex solo está pidiendo... quiero decir, _buscándose_ problemas.»[61]

El redactor daba en el clavo. La venganza llegó en forma de… ¿lo has adivinado? ...una campaña DDoS. Alguien tomó la iniciativa de eliminar a Aiplex, casi con toda seguridad recurriendo a una botnet. Golum y el resto de Anons, que se habían fijado como objetivo protestar contra el ACTA mediante la utilización de campañas DDoS, aprovecharon esta oportunidad para cambiar el rumbo de su atención y de sus energías, orientándolas hacia este asunto. Quizás no debiera sorprender que golum y sus seguidores no mostraran reparo alguno en ignorar el ACTA, cambiar de objetivos y encontrar una nueva fecha de inicio gracias a otro mordisco de oportunidad casual, como en aquella primera tirada de dados.

En uno de los primeros posters de propaganda de la Operación Venganza, esta nueva célula de Anonymous reconoció que la campaña DDoS se lanzaba «antes de lo previsto» debido a un descubrimiento inesperado realizado por un solo individuo. Los activistas luego pronosticaron, «esta será una exhibición de sangre tranquila y coordinada. No tendremos piedad». Anonymous se despedía con descaro: "BUENA CACERÍA".

¿Fue la "cacería", como anunciaba el cartel, una punzada táctica tranquila y coordinada en la que Anonymous no mostró ninguna piedad? Algo parecido. Pero, como veremos enseguida, las primeras semanas de la campaña fueron bastante caóticas, debido en parte a que la afluencia de simpatizantes fue considerable, al menos para los estándares de la época. Con tanta gente, resultaba difícil proceder de manera tranquila y coordinada. La primera campaña se lanzó el 17 de septiembre de 2010 y tuvo como objetivo el sitio web de la MPAA, al que dejaron inactivo durante casi dieciocho horas.[62] Durante los cuatro días siguientes, Anonymous atacó, entre otros objetivos, a la Federación Internacional de la Industria Fonográfica, a Aiplex (naturalmente), a la RIAA y a ACS:Law, un bufete de abogados del Reino Unido que representaba a la industria de los derechos de autor. Desde la perspectiva de estos Anons renegados, la Operación Venganza fue un éxito rotundo y en los medios de comunicación se acumularon los artículos.

Uno de los hechos destacables de la Operación Venganza fue cómo se las ingenió AnonOps, utilizando sólo material de propaganda, para convencer a los medios de comunicación (¡y a muchos de sus propios miembros!) de que la MPAA había contratado a Aiplex; no existe ninguna

prueba que avale esta afirmación. En cambio, hoy está muy extendida la convicción de que Aiplex había sido contratada por la industria cinematográfica de Bollywood. El 20 de septiembre de 2010, un buen número de respetables agencias de noticias, incluida Reuters, publicó declaraciones en esta línea, a pesar de la frágil —inexistente, en realidad— evidencia: «MPAA.org y el sitio web de Aiplex Software, una empresa que la MPAA contrató para que atacase sitios donde la piratería era generalizada, quedaron inactivos durante gran parte del día, según el blog de piratería TorrentFreak.»[63] Como la noticia recibió una cobertura tan amplia en los medios de comunicación, yo misma repetí esta trola en incontables ocasiones. A día de hoy no puedo determinar quién la propuso primero ni si nació de una confusión honesta (muchos de los principales participantes así lo creyeron realmente) o se trató de una falsedad intrigante. Sea el caso que sea, Anonymous aprovechó esta novedosa especialidad en el arte de engañar a los medios de comunicación.

Después de unos días de actividad de la operación, AnonOps estaba muy cerca de lo que sería uno de los ataques más exitosos de la temporada y en el que, por cierto, no mostraría piedad ninguna. La organización elegida, ACS:Law, sería humillada y despedazada gracias a la primera filtración importante de Anonymous.

«Me preocupa mucho más el hecho de que mi tren llegue con diez minutos de retraso… que no que estos tíos me hagan perder el tiempo con esta clase de basura»

Para el improvisado equipo reunido bajo los auspicios de la Operación Venganza, la MPAA se convirtió en el objetivo predilecto evidente. Pero el 21 de septiembre Anonymous dejó de poder desactivar eficazmente el sitio de la organización. La MPAA había aplicado una resistente protección contra los ataques DDoS empleando para ello a una empresa externa. De este modo, el 21 de septiembre de 2010, tras un intenso debate interno, Anonymous decidió dirigir su atención hacia ACS:Law, el bufete de abogados británico famoso por enviar cartas amenazadoras de parte de titulares de derechos de autor a miles de supuestos usuarios que compartían

archivos, exigiéndoles dinero y el cese inmediato de unas descargas manifiestamente ilegales. A Anonymous le llevó mucho más tiempo elegir a ACS:Law como objetivo (dos horas) que el que le llevó desactivar el sitio web de la firma (dos minutos). Tras el ataque, el director del bufete, Andrew Crossley, estaba tan poco impresionado que respondió rápidamente con la siguiente declaración: «Solo estuvo inactivo unas pocas horas. Me preocupa mucho más el hecho de que mi tren llegue con diez minutos de retraso o tener que hacer cola para tomar un café que no que estos tíos me hagan perder el tiempo con esta clase de basura.»[64]

Pero resulta que estas pocas horas de desactivación del sitio web le iban a costar a Andrew Crossley su bufete. El equipo del sitio web de ACS:Law era tan incompetente que al restaurar el sitio hicieron accidentalmente una copia de seguridad total, repleta de correos electrónicos y contraseñas, perfectamente visible para cualquiera que tuviese una pizca de capacidad técnica. Anonymous advirtió esa circunstancia, la aprovechó y cargo rápidamente todos los correos electrónicos en The Pirate Bay. Era la primera de una serie de espectaculares filtraciones dirigidas por Anonymous que aportaban pruebas de una grave falta de ética empresarial.

Para entonces el bufete de Crossley ya estaba bajo vigilancia del gobierno. Unos meses antes, el periodista especializado en tecnología Nate Anderson informó sobre un "animado debate" entre miembros de la Cámara de los Lores. Mientras discutían una enmienda llamada "Recurso contra amenazas infundadas de infracción contra los derechos de autor", muchos lores se mostraron críticos con los métodos empleados por ACS:Law.[65] Lord Lucas, que había propuesto la enmienda, pronunció palabras especialmente duras contra ACS:Law: «También debemos actuar respecto de la cuantía de daños que se pretende establecer. En un procedimiento civil sobre una cuestión de naturaleza técnica equivale a chantaje; el coste de defender una de estas cuestiones se calcula en 210.000 libras esterlinas.»[66]

Los correos electrónicos obtenidos por Anonymous simplemente contribuyeron a confirmar, con un nivel de detalle mucho más minucioso e incriminatorio, la implacable persecución emprendida por el bufete a supuestos infractores de derechos de autor en nombre de asociaciones de derechos de la propiedad intelectual.[67] Una de las prácticas empleadas incluía escribir a hombres casados acusándoles de haber descargado

material pornográfico homosexual; muchos de estos hombres pagaron entre quinientas y seiscientas libras esterlinas para desembarazarse de ACS:Law.[68] Los correos electrónicos filtrados fueron un golpe final decisivo y, en febrero de 2011, ACS:Law había cerrado.[69]

Es importante subrayar, una vez más, que la decisión de AnonOps de poner en el punto de mira a ACS:Law, como muchas de sus decisiones, se tomó en el calor del (caótico) momento. Si el grupo hubiese votado de otra manera, la operación nunca se habría llevado a cabo. Conviene echar un vistazo a la forma en que funcionan estos mecanismos de votación, y la elección de ACS:Law como objetivo constituye un ejemplo perfecto.

El canal público #savetpb (Save the Pirate Bay, que posteriormente se convertiría en #operationpayback) alojó, en su momento de mayor esplendor, a más de un millar de participantes. Muchos de ellos procedían de 4chan, donde se propagaron las noticias relativas a los métodos empleados por Aiplex e impulsaron a muchos a la acción. A los que participaban en canales públicos se les animó a que empleasen una herramienta llamada “Low Orbit Ion Cannon” (abreviado LOIC), subtitulada ”Cuando los arpones, los ataques aéreos y las armas nucleares fracasan”. LOIC es una aplicación de código abierto que permite a los usuarios contribuir de manera individual a una campaña DDoS desde la comodidad de sus hogares, accediendo simplemente a la dirección del objetivo y haciendo clic en la tentadora tecla gigante marcada “IMMA CHARGIN MAH LAZER” (“ESTOY CARGANDO MI LÁSER”). Al acceder a una dirección de IP identificada dentro de un canal, los usuarios podían dirigir sus ordenadores para unirse a un coro de manifestantes enviando solicitudes a un objetivo. Como alternativa, los participantes podían colocar a LOIC en “modo colmena”, lo que permite a los ordenadores contribuir de manera automática a la botnet voluntaria.

Mientras tanto, en el canal privado denominado originalmente #savetpb-mods y muy pronto rebautizado como #command, otros internautas participaron en un debate profundo, a menudo acalorado y absolutamente confuso relacionado con la estrategia y los objetivos. La mayoría de los participantes en el canal público ignoraba la existencia de este canal privado, a menos que formasen parte de la minoría que finalmente aprovechó la ocasión para unirse a él. Durante una entrevista, uno de los fundadores del canal secreto explicó el criterio de selección de la

siguiente manera: «Eres invitado por otro miembro de #command si has demostrado ser productivo/útil o digno de confianza.»

A continuación incluyo una mínima muestra de extractos de una conversación de dos horas realmente enrevesada —pero, aun así, semicoherente– que tuvo lugar en #command cuando los participantes decidían poner en el punto de mira a ACS:Law. La toma de decisiones a menudo sigue un camino líquido. Empezó con los participantes destancando el impresionante número de personas reunido en el canal público y, por así decirlo, esperando órdenes:

<Anon2>: más de 660 personas
<Anon5>: eh oh
<Anon5>: el ventilador está a punto de alcanzar la mierda
<Anon6>: sí [...]
<Anon4>: el ventilador explotó de mierda
<Anon7>: su [MPAA] protección contra ddos funciona
<Anon7>: ¿sugiero que cambiemos de objetivos?
<Anon7>: ¿bpi? [Industria Pornográfica Británica]
<Anon8>: ¿por qué no riaa? [Asociación de la Industria Discográfica de Estados Unidos]
<Anon7>: porque fracasamos con bpi la última vez debido a que éramos pocos

Mientras conversaban, seguían llegando personas y comenzaron a preocuparse por el impulso y los ánimos:

<Anon1>: mientras tanto están apareciendo unos cuantos artículos nuevos diciendo que al menos causamos un montón de daño
<Anon8>: ¿qué ha hecho BPI?
<Anon7>: Bueno
<Anon9>: Tíos, no discutáis ningún drama en el chat principal.
<Anon9>: Estamos aquí por la propaganda. Arriba el ánimo. [...]
<Anon9>: Solo con que SUGIRAMOS que nuestros esfuerzos son “inútiles”, la gente se largará en masa.
<Anon9>: Siempre se ha tratado de la moral.
<Anon9>: No tenemos alrededor de 800 personas por decir la verdad.
<Anon9>: tenemos 800 personas que CREEN que están haciendo algo.
<Anon7>: Tíos, NO quiero que fracasemos a los ojos de la opinión pública o que nuestras tropas se echen a perder. Tenemos que cambiar de objetivos, pronto.

El desacuerdo sobre los objetivos iba en aumento y alguien señaló que el golpe financiero contra MPAA era insignificante ya que la organización hacía un pago global fijo por la protección contra los ataques DDoS. Finalmente, la gente accedió a suspender el ataque contra MPAA y a cambiar de objetivos. Alguien subrayó la naturaleza de este esfuerzo: «pero en cualquier caso debemos considerarlo un experimento. Demostradme que estoy equivocado.» Justo cuando los participantes pensaban que habían alcanzado un consenso, alguien insistió en que se votase; como suele ocurrir en las reuniones de IRC (y aun más con un grupo como Anonymous), la conversación se volvió incluso más enrevesada:

<Anon7>: Nooo
<Anon7>: Esperad
<Anon7>: Votemos.
<Anon8>: Ahora tenemos opinión pública porque no atacamos sitios al azar
<Anon7>: Primero, designemos los sitios.
<Anon7>: Hasta ahora se han designado riaa y bpi.
<Anon7>: ¿Algún otro?
<Anon9>: Creo que tengo la idea perfecta
<Anon7>: podemos votar.
<Anon16>: Hola.
<Anon1>: dejemos hablar a Anon9
<Anon9>:Creo que estoy de acuerdo con Anon13. ACS:Law.
<Anon9>: A saco.
<Anon9>: Pegar su sitio web de mierda, postear los artículos que hablan de ellos, etc.
<Anon9>: Si nos desviamos ahora, NO tendrán tiempo de prepararse.
<Anon1>: bueno, /b/ ¿un nuevo cartel con el objetivo de mañana, a la misma hora?
<Anon10>: Yo también estoy a favor de acs:law
<Anon4>: yo también
<Anon13>: ¿Cambiamos el tema en el chat principal y desviamos los láseres ahora, sin perder a casi nadie, o atacamos mañana perdiendo posiblemente a centenares?
<Anon8>: que alguien me dé una motivación igualmente buena para un objetivo [...]
<Anon7>: ¿votamos?
<Anon13>: yo voto por ACS.
<Anon7>: DDoS ACS:LAW. 1 = sí, 2 = no

Mientras algunos votaban, otros continuaron debatiendo largamente la elección de los objetivos, argumentando que «atacar agencias antipiratería

al azar no contribuye a nuestra causa». Esta situación provocó otra larga y tediosa ronda de votaciones. Finalmente, dos horas más tarde, parecían haberse acercado un poco a un acuerdo; pero, en medio del debate, ¿adivináis lo que pasó?

<Anon7>: www.acs-law.org.uk
<Anon12>: dame la información que te pedí.
<Anon7>: ¡www.acs-law.org.uk YA ESTÁ inactiva! [...]
<Anon12>: joder
<Anon12>: ?
<Anon1>: ¿OMG?
<Anon13>: Eso ha sido rápido.
<Anon1>: ¿cuánto tiempo nos llevó volver a votar? XD
<Anon14>: Más tiempo del que les llevó que se desactivara

Alguien debió de pensar que el consenso alcanzado era suficiente para seguir adelante y poner en marcha las botnets.

Dos horas de planificación, dos minutos de DDOseo y poco después la firma tuvo que cerrar. Poco más de un año después de que Anonymus filtrase los correos electrónicos, Crossley —que se había mostrado más preocupado por tener que hacer cola para conseguir un café— fue juzgado por el Tribunal Disciplinario de Abogados por numerosos cargos. Crossley reconoció seis de las siete acusaciones, incluidas las dos siguientes: «actuar de una manera que probablemente mermase la confianza que el público había depositado en él o en la profesión jurídica» y «utilizar su posición como abogado para aprovecharse indebidamente en su beneficio de los destinatarios de las cartas».[70] Se ordenó que pagase 76.000 libras esterlinas en concepto de multas y se le suspendió la licencia por dos años. Aunque cuestionó la afirmación de que no había tomado las medidas adecuadas para proteger los datos de los clientes, se le declaró culpable de los cargos presentados y la Oficina del Comisionado de Información también le sancionó por vulneración de datos.[71]

Aunque muchas de las acciones llevadas a cabo por Anonymous buscan simplemente atraer la atención de los medios de comunicación para airear alguna cuestión puntual, en ocasiones el destino les concede más de lo que se proponían, como la oportunidad accidental de reprimir la corrupción.

Las armas de los geeks (raramente coinciden)

Hacia finales del otoño de 2010, con el despliegue constante de técnicas digitales de acción directa, AnonOps había insuflado nueva vida a la aún incipiente idea de que Anonymous podía ser un estandarte para el activismo. El nombre, otrora asociado exclusivamente a las formas más abyectas de troleo, comenzaba lenta pero firmemente a ser asociado con una irreverente marca de disidencia. Sin embargo, los que estaban detrás de las campañas lanzadas en septiembre y octubre, como golum y los Anons citados más arriba, no pretendían existir como equipo, y mucho menos como una red, más que unas pocas semanas. Pero, como un reflejo de los acontecimientos que dieron a Chanology una discreta entidad, la cobertura de los medios de comunicación también ayudó a consolidar a este nuevo equipo. En una extraña entrevista con TorrentFreak, uno de los organizadores principales explicó el porqué:

> El mando de la operación se vio “agradablemente” sorprendido por la cobertura y atención abrumadoras de los medios de comunicación, pero se preguntó qué hacer a partir de ahí. Se convirtieron en el centro de atención pero realmente no tenían ningún plan de futuro. Finalmente decidieron continuar por el camino que de entrada les había llevado hasta allí: más ataques DDoS... La atención de los medios de comunicación fue sin duda importante para ayudar a que la operación siguiera adelante.[72]

Con AnonOps llegado para quedarse, también había signos inequívocos de que se estaba provocando una división entre diferentes nodos dentro de las ramas activistas de Anonymous. Chanology y AnonOps, las alas más activas del colectivo, no podían ser más diferentes en términos de tácticas. Una permanecía habitualmente dentro de los límites marcados por la ley, mientras que la otra se dedicaba con avidez y entusiasmo a vulnerarla. Mediante el reconocimiento de estas disputas internas e impulsos sectarios, Anonymous adoptaría finalmente la letanía «Anonymous no es unánime».[73]

Fue más o menos en esta época cuando empecé a captar la importancia global de estos geeks y hackers divergentes y dispares —Anonymous (Chanology vs. AnonOps), Assange, Manning, The Pirate Bay y otros—,

elementos todos ellos que accedían al escenario político en un número mucho mayor que nunca hasta entonces. Mediante la organización de protestas relacionadas con un amplio abanico de temas —en particular las libertades civiles— transformaron la política, la ley, las perspectivas de los medios de comunicación y la opinión pública. Aunque sin duda único en su discurso ampuloso y su carácter caprichoso, Anonymous formaba claramente parte de un manantial de hackers y geeks que estaban tomando las riendas de las cuestiones políticas y hacían oir sus voces.

Anonymous señaló la creciente importancia de lo que yo denomino "armas de los geek", en referencia a "armas de los débiles", una expresión empleada por el antropólogo James Scott en 1985 en su libro del mismo nombre, para referirse a la singular naturaleza clandestina de la política campesina. Mientras que *Weapons of the Weak* describe las tácticas que utilizan las poblaciones económicamente marginadas que participan en actos ilícitos a pequeña escala —tales como la lentitud intencionada en el trabajo o el vandalismo— que no parecen tener un carácter político evidente, "armas de los geek" es una modalidad de la política ejercida por una clase de actores visibles y privilegiados que a menudo ocupan el centro de la vida económica.

La tecnología no determina de manera simplista la política del hackeo, aun cuando las experiencias tecnológicas habitualmente conformen su expresión. Así como existen muchas maneras de practicar el hackeo, existen también muchas maneras de que los hackers accedan al escenario político. Desde la elaboración de políticas hasta la participación en partidos pirata, desde reinventar la ley mediante software gratuito hasta llevar a cabo arriesgados actos de desobediencia civil, los geeks y hackers no están vinculados a un único sentimiento político, como el liberalismo, y ciertamente no coinciden en la forma en que debería producirse el cambio social.

Lo que todos ellos tienen en común es que sus herramientas políticas, y en menor grado sus sensibilidades políticas, surgen de las experiencia concretas de su oficio, como administrar un servidor o editar vídeos. A menudo, estas habilidades se canalizan hacia actividades específicas con el fin de reforzar las libertades civiles, como en el caso de la privacidad. A diferencia de los campesinos que buscan permanecer en un segundo plano y anónimos incluso como grupo, los geeks y los hackers —incluso los

anónimos Anonymous— llaman explícitamente la atención sobre ellos a través de sus actos políticos volátiles y habitualmente controvertidos. En otoño de 2010, AnonOps se encontraba a la vanguardia de las pruebas y los experimentos que buscaban indagar las nuevas posibilidades y limitaciones legales de la desobediencia civil digital.

Y mientras que algunos consideraban un éxito estos experimentos, otros —incluso aquellos alineados con la lucha por las libertades civiles— se mostraban cautelosos ante las tácticas empleadas. El Partido Pirata en particular estaba menos que entusiasmado con respecto al uso político del DDoS. El Partido Pirata es un partido político que ha realizado incursiones en Europa y Australia (y afirma contar con una base muy débil en Norteamérica). Lo creó en 2006 Rickard Falkvinge, el defensor sueco de la cultura libre, y actualmente su programa está basado en la reforma de los derechos de propiedad intelectual, la exigencia de libertades civiles y en Internet, y la elaboración de herramientas para apoyar la democracia directa. Los partidos pirata en el Reino Unido y Estados Unidos escribieron una carta a AnonOps solicitando el cese inmediato de la actividad DDoS. (Cabe señalar que la carta no solo provocó un intenso debate entre los participantes de AnonOps sino también entre los propios miembros del Partido Pirata.)[74]

> La Operación Venganza debe acabar. Si bien es sin duda una señal el hecho de que un número creciente de personas se sienta frustrado por la manera en que las leyes se modifican constantemente para destruir nuestra cultura creativa en nombre de la preservación de la rentabilidad, sus métodos producen efectos más negativos que positivos en el esfuerzo global.
>
> Al proseguir con los ataques de la Operación Venganza dificultaréis la acción de quienes promueven la reforma de los derechos de propiedad intelectual y la restricción de los abusos de los derechos de autor, pero que lo hacen dentro de los límites de la ley. En lugar de ser capaces de argumentar en favor de una reforma legislativa de la propiedad intelectual por sus propios méritos, se les acusará de defender a delincuentes y de promover la desobediencia de la ley. A los legisladores y los medios de comunicación les resultará más fácil

> ignorar los evidentes beneficios derivados de derechos de autor justos y de la libre expresión para reclamar una legislación más dura con el fin de «detener a esos piratas y hackers».[75]

Sorprendentemente, por un período de tiempo muy breve los participantes en la Operación Venganza que formaban parte de #command, se tomaron en serio el llamamiento del Partido Pirata e incluso consideraron abortar el uso de tácticas ilegales en favor de un estilo más moderado y reformista: el anticipo de una lista de exigencias. La entrevista a Torrent Freak reveló públicamente la existencia del canal secreto #command y confirmó la nueva adscripción de los participantes a tácticas respetuosas con la ley. A continuación se reproducen algunos extractos clave de la mencionada entrevista:

> El grupo principal está en el canal #command en IRC. Este grupo principal no es más que una especie de intermediario entre la gente que participa en ese canal de IRC y el verdadero ataque. Otro grupo de personas en el IRC (el canal principal #operationpayback) solo está allí para disparar sobre los objetivos...
>
> La semana pasada #command decidió ralentizar los ataques DDoS y optar por otra estrategia, principalmente recuperar el foco de atención. Se tomó la decisión de hacer una lista de peticiones dirigidas a los gobiernos de todo el mundo. En un gesto contrario a los deseos de las influencias anárquicas, el grupo de mando decidió participar en la discusión política.[76]

Esta noticia dual —que existía un canal secreto y que sus miembros querían ser "legales"— fue mal recibida por el canal de cara al público #operationpayback en AnonOps. El resultado fue, básicamente, un motín. "Gobo" (no es su seudónimo real), un importante participante activo en el canal público —quien más tarde se convertiría en miembro de otro canal independiente y secreto catalizado de nuevo por esta revelación— explicó:

> Ese artículo irritó seriamente a mucha gente en el canal principal. Se produjeron grandes discusiones sobre el hecho de que Anonymous

> carecía de liderazgo y «quién coño se creen que son». De alguna manera #command no percibió realmente la profunda controversia que estaba generando al sobrepasar los límites de su propósito (según definió el participante en el canal principal).[77]

Poco sabían los quejumbrosos Anons que existía otro canal, *incluso más secreto*, llamado #internetfeds. Creado originalmente con la finalidad de ejecutar operaciones —sobre todo actividades de hackeo encubiertas— había permanecido inactivo durante algún tiempo. Uno de sus miembros se puso en contacto con Gobo y le invitó a unirse a #internetfeds con un plan para reactivarlo. El compromiso público de un cese de los ataques de DDoS pareció de pronto muy dudoso:

> Esencialmente, su filosofía era la siguiente: la Operación Venganza «abandonaría públicamente toda actividad ilegal» de conformidad con la carta del partido pirata. #internetfeds llevaría a cabo estas actividades de forma privada y en nombre de “Anonymous” pero *no* en nombre de la Operación Venganza, y su existencia permanecería sagradamente secreta para no poner en peligro la nueva imagen de “protesta legítima” que #command quería darle a la Operación Venganza.[78]

De modo que un pequeño equipo dentro de un pequeño grupo conspirador planeaba reavivar otro grupo conspirador aún más pequeño y secreto, comprometido solo con el principio rector, como en *El club de la lucha*[*], de mantener un absoluto silencio con respecto a su existencia (es posible que el grupo operase en secreto, pero cada uno de sus *defacements* estaban acompañados de un logo que incluía su nombre: “Pwned por #internetfeds”)[79] Pero resultó que #internetfeds nunca tuvo que llevar a cabo esta misión “sagradamente secreta” que se había propuesto porque los participantes del canal principal básicamente mandaron a la mierda a #command y reafirmaron su intención de continuar con los ataques DDoS con o sin ellos: la “guerra civil” estalló en el canal público donde, según Gobo, la mayoría de la gente

> condenaba abiertamente no solo la idea de actuar de manera legal, sino

> específicamente el hecho de que #command se hubiera mostrado tan absolutamente líder-fagged al acceder a todo esto sin siquiera mencionarlo al canal principal. Se produjo una discusión extremadamente agria y, a continuación, alguien le dijo simplemente a la gente que se olvidaran de la colmena #loic y atacasen manualmente el siguiente objetivo, con o sin el apoyo de #command.[80]

Aquellos que formaban parte de #command escucharon a las airadas masas de IRC y «casi inmediatamente dieron marcha atrás en su compromiso de que las operaciones fuesen legales», explicó Gobo. Aunque #internetfeds ya no era un elemento técnicamente necesario para este DDoS particular (ya que #command había enderezado el rumbo del DDoSeo gracias a la presión ejercida por los integrantes del canal público), continuó activo de todos modos, convirtiéndose finalmente en «un canal de filtraciones y *defacement* extremadamente militante», según la descripción de Gobo, que realmente brillaría en los meses siguientes. La paz se había restablecido, pero se sostenía con pinzas.

Legitimidad frente a legalidad

En septiembre de 2010, cuando surgió un nuevo nodo de Anonymous de la justificada indignación por la doble negociación de la industria de la propiedad intelectual, todo parecía encontrarse siempre a punto de explotar. La acción era a menudo acalorada, confusa, conmovedora y espontánea, como las emociones experimentadas por los participantes. AnonOps se había vuelto cada vez más reflexiva en su proceso de toma de decisiones como consecuencia directa del pensamiento colectivo sobre la cuestión de la propia colectividad. El tema de la organización, indudablemente, era subrayado por muchos participantes molestos por el doble rasero aplicado durante las campañas iniciales. Uno de los principales hackers me explicó por qué se sentía justificado a seguir adelante con estas tácticas ilegales, un sentimiento que parecía representar el ánimo general del momento: «Lo consideraba una forma de justicia poética en respuesta al ataque DDoS de Airplex contra Pirate Bay.» Gobo, que había trabajado estrechamente con golum, destacó cómo él siempre

> hablaba apasionadamente sobre el hecho de que gente que había conocido de Anonymous [había sido arrestada por tomar parte en ataques DDoS basados en el troleo], y sin embargo aquí había gente importante del mundo empresarial presumiendo de ello, pero todo el mundo sabía perfectamente que nadie les acusaría jamás. Golum sostiene firmemente que no debería existir un doble rasero en la política, de modo que para él se trataba de que «las corporaciones se van de rositas» con delitos que la gente común siempre debe pagar.[81]

En noviembre este tipo de sentimientos individuales se transformó en una declaración política colectiva. Poco tiempo después de que AnonOps se retractase de su compromiso de pasar a la legalidad, el grupo publicó una carta dirigida al Partido Pirata. El texto incluía una sofisticada justificación del DDoS que se centraba en la cuestión de la legitimidad frente a la legalidad. Éste es un extracto de la carta:

> Anonymous y la Operación Venganza comparten valores y objetivos —es decir, libertad de información, expresión e intercambio— con los partidos pirata, pero somos entidades absolutamente independientes.
>
> Nos estamos preocupados por la legalidad sino por la legitimidad. Los que deciden nuestras leyes son los mismos que decidieron que el acoso a la propiedad intelectual pública, la erosión de las libertades civiles y las aberraciones de censura tales como COICA, ACTA y la DEAct son cosas buenas y justas para hacer cumplir al pueblo. Ellos lo hacen al tiempo que aplican de manera selectiva sus propias leyes cuando se trata de organizaciones “oficiales” que dirigen una operación de chantaje (demandando conscientemente a miles de personas por infringir la ley con pruebas falsas) o realizar ataques DDoS a sitios contrarios a sus intereses (AiPlex). Debido a esta muestra de absoluta hipocresía nosotros no reconocemos su “autoridad”.
>
> Por último, reconocemos y respetamos la labor que hacen los partidos piratas y les deseamos suerte. Esperamos que todos continuéis vuestra lucha, como nosotros continuamos la nuestra.[82]

Tal como indica esta carta, AnonOps se sentía perfectamente cómodo disfrazando sus actividades de desobediencia civil. Poco después de haber llegado en noviembre a un consenso ético en cuanto a los ataques DDoS, los números en su servidor de IRC descendieron bruscamente. Solo permanecieron unas cuantas élites secretas dispersas, inmovilizadas en sus canales autónomos y clandestinos. Resultaba imposible prever que, apenas tres semanas más tarde, lanzarían la mayor campaña DDoS de desobediencia civil que el mundo había visto jamás.

Capítulo 4

El disparo que resonó en todo el mundo

Solo tengo un minuto,
Solo sesenta segundos en él.
Impuesto sobre mí, no puedo rechazarlo,
No lo busqué, no lo elegí,
Pero usarlo depende de mí.
Debo sufrir si lo pierdo,
Dar cuenta si abuso de él
Solo un pequeño minúsculo minuto,
Pero en él se halla la eternidad.

—Benjamin Elijah Mays,
Educador estadounidense y presidente
del Morehouse College

A menudo los comentaristas describen a Anonymous como una entidad amorfa que existe en una suerte de estado gelatinoso mítico y primordial del no-ser que solo adquiere una existencia sólida cuando un agente externo pronuncia su nombre. Aceptando esta lógica, algunos escritores sugieren que Anonymous y sus intervenciones sufren de una inherente falta de cohesión. «El mensaje confuso del grupo, sin portavoces, líderes o planes

políticos concretos que proporcionen una dirección estable —escribió Art Keller en *Newsweek*—, se ve agravado por una ideología que oscila entre la extrema izquierda, la extrema derecha y las principales preocupaciones de los ciudadanos.»[83] Un ejemplo más prosaico procede de un Anon que me hizo el siguiente comentario durante una conversación personal por chat: «Hoy he hablado con un amigo de la vida real sobre Anonymous y parecía tener la misma visión de cerebros incorpóreos mantenidos en suspensión que orbitan alrededor de la tierra en satélites de combate, o algo así; la idea de que hubiera gente de carne y hueso implicada parecía desconcertarle.»

Estas generalizaciones —divulgadas tanto por los medios de comunicación como por la gente corriente— no solo son erróneas sino que nos alejan de una verdadera comprensión de Anonymous. Lejos de carecer de estructura o de brincar locamente como la aguja de una brújula en el polo norte, Anonymous incorpora numerosas relaciones, estructuras y actitudes morales. Los seres humanos —hablando, codificando, debatiendo, discutiendo, creando y actuando— están allí a cada paso del camino. Este sentimiento encontró una expresión particularmente agradable durante una conversación que mantuve con Mustafa Al-Bassam, un famoso ex miembro de LulzSec, un grupo de hackers que más tarde se escindió de Anonymous. Exasperada por los intentos de catalogar cada canal secreto y recopilar cada nota relevante, un día le encontré en línea y le pedí —le rogué, en realidad — que me proporcionara un lista limpia, ordenada y definitiva de todos los canales que pudiera recordar. Él accedió amablemente y, en medio de su meticulosa explicación, que aun así me dejó confusa, preguntó, «¿Conoces kittencore?»

*Oh, joder, ¿kittenporn (*porno con gatitos*)?*, pensé. Afortunadamente, él refrenó mi imaginación y aclaró: «El canal de IRC; teníamos un canal llamado #kittencore y otro llamado #upper-deck. La única diferencia es que en #upperdeck estaba la misma gente que en #kittencore salvo una persona.» Le pregunté por qué mantenían a una persona en la oscuridad. Me contestó, «porque se incorporó muy tarde y éramos reacios a mantenerle en el centro, y también porque llegó justo cuando estábamos repartiendo los bitcoins».

«Micro-micro-política y cábalas acurrucadas dentro de cábalas», contesté.

Es precisamente esta mezcla de concreción y abundancia —un canal

igual a otro, menos una persona, puesto que es demasiado nueva y aún no es digna de fiar— lo que hace de Anonymous algo tan difícil de describir y a la vez tan difícil de encasillar en una plantilla mental prefabricada. La presión y el deseo de anonimato permite que los participantes, en su conjunto, representen una mezcla de sus almas, conjurando la existencia de algo siempre emergente y en flujo continuo. La cantidad de relaciones, feudos y camarillas en una existencia simultánea es en gran parte invisible al público, que tiende a observar a Anonymous desde el punto estratégico de una propaganda cuidadosamente esculpida y de la mirada bastante previsible de los medios de comunicación.

Y, sin embargo, atisbando a través del ordenador vemos que Anonymous es como un gran saco colectivo de carne—acoplado mediante cables, transistores y señales de WiFi— repleto de miles de canalizaciones que bombean sangre, kilos de vísceras llenas de fluidos vitales, un conjunto de cables de alta tensión, sostenido por una estructura ósea con pistones musculares sujetos a ella y dirigido desde una cúpula cavernosa donde se aloja un centro de control incansable; la analogía de estos sistemas fabulosamente grotescos y caóticamente precisos que, si se desmonta, se convierte en lo que llamamos gente. Anonymous no es muy distinto de nosotros. Consiste simplemente en un grupo de seres humanos sentados ante sus pantallas brillantes y con los dedos desplazándose sobre el teclado, como los seres humanos acostumbran hacer en este preciso momento en el largo arco de la condición humana. Cada cuerpo tomado individualmente aporta el vector para una historia singular compleja e irreductiblemente única –que refleja en su aislamiento la complejidad de todos los fenómenos sociales en su conjunto—, que puede a su vez ser reducida aún más al orden de los acontecimientos: simples vuelos de dedos y un ocasional gesto del ratón que se expresan en otra parte, en una pantalla, como un texto bidimensional o un vídeo tridimensional; la canción que interpretan esos dedos sobre los teclados resuena en una sinfonía bien orquestada aunque cacofónica y a menudo discordante; es cantada en la estrofa más básica e impúdica, atonal y plana, pero fascinante para muchos: la épica mítica de Anonymous.

Anonymous no ha sido siempre un colectivo tan complejo; no fue hasta finales de 2010 que el grupo activista se convirtió en un laberinto tan enredado y en constante cambio. En noviembre de 2010, el minotauro que

dominaba el laberinto de Anonymous aún no había encontrado su vía de escape hacia el mundo, pero se estaba acercando a ella. Chanology se mantenía activa y el IRC de AnonOps seguía siendo el centro neurálgico para un carrusel de campañas de DDoS dirigidas contra la industria de la propiedad intelectual. Hacia finales de noviembre, este flujo continuo de acción directa en apoyo del intercambio de archivos se detuvo bruscamente. La participación en los canales de IRC de cara al público se redujo a un mínimo histórico. Pero los equipos principales, que habían colaborado en los canales privados, no cerraron silenciosamente sus puertas y bajaron las persianas (si bien esas cifras bajas no dejaban de preocuparles). En cambio buscaron organizarse mejor. Una sesión de intercambio de ideas produjo un documento escrito colectivamente en el que ponían de manifiesto la finalidad y la estructura del canal privado #command, cuyas normas se habían dado a conocer previamente en noviembre (*véase* el recuadro en la página siguiente), escandalizando a amplias filas de Anonymous.

El documento, que existía en diversos y llamativos estados, definía en primer lugar el papel limitado de #command al «actuar como un intermediario» que «no toma decisiones solo» y debe guiar «solamente la discusión, no la dirección» de las operaciones. El documento finaliza con una lista de reglas, incluida la irónica declaración de que «solo los adultos» están autorizados a estar «al mando». Irónica declaración ya que había muchos individuos menores de dieciocho años (y ¿de verdad asociaba a Anonymous con “adulto”?).

En este documento aparecen muchos conceptos que probablemente les resulten poco familiares a los vírgenes en IRC y podrían merecer alguna explicación. Primero: utilizas a un cliente de IRC para conectarte a un servidor y luego escoges un handle o “apodo”, que puede ser tu nombre legal pero que habitualmente es alguna otra cosa. Tienes la opción de hablar mediante chat con otros usuarios conectados, o puedes unirte a “canales”, que están indicados mediante un signo (#), y a los que se puede unir cualquier usuario que conozca la existencia de la sala, siempre que no se trate de una sala a la que se acceda solo por invitación. Una vez que te has unido a una sala, hablas con otros usuarios que están allí, habitualmente sobre algún tema específico del canal. Quienquiera que haya creado el canal se llama el “fundador del canal” y tiene cierto poder para cambiar sus propiedades, determinando quién puede entrar, si el canal es visible en la

lista de canales públicos del servidor, etcétera.

Reglas en el mando:

- Nadie echa y, desde luego, nadie prohíbe dentro del mando.
- No interrumpes a los demás.
- Se señalan primero los asuntos en cuestión, luego las prioridades.
- La gente que trolea en el mando es expulsada (permanentemente) de la lista AOP.
- Las disputas personales son tabú.
- Adultos solamente.
- Ningún tema offtopic en las discusiones (del staff).
- Señala los problemas de una manera estructurada: nombra el problema, sugiere la solución. Si no puedes plantear una solución, entonces al menos ofrece una prueba o argumenta tus afirmaciones, siempre que tu argumento sea válido.
- Si no te gusta alguien, supéralo. En esto estamos todos juntos.
- Los administradores/Operadores se consideran un ejemplo. ¡Actúa según ese comportamiento!
- No esperes que los operadores de IRC resuelvan todos tus problemas, inténtalo tú y, si todo lo demás falla, ¡pregunta a los operadores (OP)!

Los operadores también pueden otorgar poder a otros —al menos en algunas versiones de IRC— añadiéndoles a lo que se denomina lista “AutoOp (AOP)”. Cualquiera que se encuentre en esa lista puede “echar” a alguien del canal por cualquier motivo que elija, e incluso prohibirle que regrese. En un estrato de poder superior están los IRCops —una fracción que dirige el servidor y tiene el poder no solo de echar a la gente de los canales individuales, sino también del propio servidor, desconectándoles totalmente. Los IRCops tienen también la capacidad de alterar las configuraciones de los canales individuales y desarrollar muchas otras funciones de carácter administrativo. Habitualmente hay muchos operadores de canales individuales pero pocos operadores de servidores de IRC. Para muchos IRCops, intervenir en cualquier disputa en un canal individual es un ejercicio frustrante que requiere juzgar hechos de los que no tienen información. Como consecuencia de ello, las decisiones relativas

a un canal se derivan habitualmente a los operadores de los canales, con la intervención de un administrador del servidor solo en circunstancias extremas.

Muchos participantes extrajeron (o al menos *intentaron* extraer) principios sensatos de orden del IRC y de otros sitios de interacción estables. Este orden, sin embargo, es delicado y precario, siempre al borde del desorden. Pero, como sucede con tantos escenarios de agitación embaucadores, estos momentos de caos no conducen necesariamente a la ruptura y al inmovilismo. En cambio funcionan a menudo como comienzos, necesarios para la vitalidad e incluso la regeneración de la comunidad más amplia. La yuxtaposición de dos citas, una del filósofo español George Santayana y otra de Henry Brooks Adams, pone de relieve esta lección:

> Caos es el nombre de cualquier orden que produce confusión en nuestras mentes, pero no será caos una vez que lo veamos por lo que es.
>
> El caos con frecuencia genera vida, cuando el orden genera hábito.

En la bastante enrevesada historia que estoy a punto de relatar quedará clara la forma en la que Anonymous, como la mayoría de los movimientos sociales, permanece abierto al azar y al caos. La diferencia reside en que Anonymous se muestra tal vez solo un poco más abierto a la mutación. No hay demostración más palpable de esta característica que lo ocurrido a comienzos de diciembre de 2010, cuando una decisión caprichosa puso fin a un período de inactividad en el seno de AnonOps, abriendo la puerta de par en par a nuevas posibilidades prácticas y permitiendo la incorporación de numerosos recién llegados como reclutas preparados para la acción (en su mayoría ignorantes, nuevamente, de la existencia del todavía privado canal de IRC #command). Esta decisión contribuyó a revitalizar a AnonOps hasta tal punto que la red de IRC del grupo se convirtió en una fuente de incesante actividad durante más de un año, superando a WikiLeaks como centro de activismo hacker más importante en Internet.

Pero, antes de que describamos esta decisión caprichosa, haríamos bien en recordar su tristemente célebre resultado: el apoyo de AnonOps a WikiLeaks a través de una masiva campaña de DDoS a raíz de la revelación

más polémica realizada por esa organización denunciante. El 28 de noviembre de 2010, WikiLeaks difundió públicamente 220 de 251.287 cables diplomáticos estadounidenses clasificados, la mayor filtración de material clasificado jamás realizada, programada para que coincidiera con análisis profundos realizados por *The Guardian*, *The New York Times*, *El País*, *Le Monde* y *Der Spiegel*. El gobierno de Estados Unidos enfureció y un trío de poderosas empresas —Amazon, MasterCard y PayPal (entre otras)— cedieron a su influencia y se negaron a procesar las donaciones o acoger en sus sitios web a la sitiada organización.

Aunque WikiLeaks ya había publicado cientos de miles de documentos militares sobre las guerras de Afganistán e Irak, que rebosaban de revelaciones sobre escuadrones de detención, bajas civiles, la utilización de prostitutas infantiles y un sinnúmero de otros horrores, el “Cablegate” consiguió un lugar de privilegio en este panorama. Dejó al descubierto no solo las conversaciones intradiplomáticas que normalmente permanecen ocultas detrás de un velo de protocolo diplomático, sino también —e incluso de un modo más lascivo— las discusiones internas y la recopilación de información de los propios diplomáticos estadounidenses. En 2009, la entonces Secretaria de Estado, Hillary Clinton, según supimos, fusionó diplomacia y espionaje en una única actividad, ordenando a los funcionarios del servicio diplomático de Estados Unidos que recogiesen números de tarjetas de crédito, números de viajeros frecuentes e información biométrica de los funcionarios extranjeros. Nos enteramos entonces de que la Administración Obama había dirigido en secreto una guerra en Yemen y lanzado ataques con misiles contra sospechosos de terrorismo, mientras el gobierno yemení encubría estas actividades adjudicándose la responsabilidad de las acciones. Descubrimos que los servicios de inteligencia de Estados Unidos creían que Corea del Norte había entregado a Irán diecinueve de sus misiles de gran alcance, que, por de pronto, la opinión pública ni sabía que existían. Supimos que los líderes de Arabia Saudita habían presionado a Estados Unidos para que bombardease Irán con el propósito de «cortar la cabeza de la serpiente», tal como lo expresó el propio rey Abdullah. Los cables mostraban que Israel se estaba echando un farol con sus amenazas de lanzar ataques aéreos contra Irán, y que Estados Unidos participaba en negociaciones criminales con el hermano corrupto y traficante de drogas del presidente afgano Hamid Karzai. Estos cables

también abordaban cuestiones comparativamente banales, como las críticas y los insultos rutinarios de los diplomáticos estadounidenses dirigidos a líderes extranjeros.[84] Antes las cosas eran simplemente interesantes y provocativas, pero ahora, con la aparición de estas nuevas revelaciones, la opinión pública descubrió que sus bocas podían abrirse cada vez más, como si estuviesen sujetas a algún artilugio ortodóncico invisible, accionado manualmente por el propio Julian Assange.

Sarah Palin sugirió que Assange fuese perseguido «con el mismo rigor con la que perseguimos a al-Qaeda y a los líderes talibanes».[85] El senador Joe Lieberman declaró que se trataba de «una acción escandalosa, temeraria y despreciable que socavará la capacidad de nuestro gobierno y nuestros socios para mantener a nuestro pueblo seguro y trabajar juntos para defender nuestros intereses vitales».[86] El personal de Lieberman se comunicó con Amazon —no solamente el mayor vendedor de libros del mundo sino también su mayor anfitrión de web— y le pidió que excluyera a WikiLeaks de sus servidores. La empresa accedió. Las firmas financieras que procesan transacciones con tarjetas de crédito en todo el mundo siguieron su ejemplo, cortando el cordón umbilical entre los donantes y WikiLeaks. Aunque WikiLeaks no había sido declarado culpable de nada por ningún tribunal de justicia, estas empresas, sin ninguna obligación legal de hacer lo que el gobierno les pedía, siguieron adelante de todos modos. Anonymous estaba indignado.

Dos semanas más tarde, AnonOps se convirtió en la zona cero para llevar a cabo la mayor campaña individual de acción directa que Internet había… y aún ha visto jamás, al menos medido por número de participantes. Más de siete mil internautas se conectaron al canal de IRC de AnonOps, #operationpayback, para echarles una mano, animarles o simplemente observar. Siete mil usuarios en un solo canal sigue siendo la mayor congregación humana individual en un canal de IRC jamás conseguida.[87] Fue una «demostración masiva contra el control», como el hacker de software libre Richard Stallman describió el evento en un editorial del *The Guardian*.[88] Solo en el mes de diciembre, LOIC fue descargado 116.988 veces, mucho más que durante las primeras campañas de DDoS.[89] Mientras que solo una fracción de aquellas personas estaban conectadas efectivamente a la colmena de Anonymous, el interés por la herramienta estaba alimentado sin duda por las informaciones acerca de las

actividades desarrolladas por Anonymous.

La atención prestada por los medios de comunicación era frenética y catapultó a este colectivo de colectivos de oscuridad relativa al centro del escenario internacional. No solo los sospechosos habituales —las publicaciones y los blogs de tecnología— informaron sobre la rebelión, sino que también lo hicieron la mayoría de los principales noticiarios nocturnos. La CNN invitó al estratega digital Nicco Mele, que elogió a Anonymous durante una entrevista en profundidad. En *The New York Times*, uno de los santos patrones originales de Internet, John Perry Barlow, definió la campaña de Anonymous como «el disparo que resonó en todo el mundo; esto es Lexington».[90]

WikiLeaks y Anonymous parecían una combinación ideal. La campaña de DDoS de Anonymous selló esta alianza a través de un despliegue espectacular de apoyo y solidaridad. Pero, como se ha indicado anteriormente, la decisión de AnonOps de intervenir se produjo de un modo bastante desordenado y complejo. La periodista Parmy Olson, en su libro *We Are Anonymous*, describe como sencilla la decisión de AnonOps de prestar su apoyo a WikiLeaks:

> La gente que formó AnonOps estaba hablando sobre la controversia creada por WikiLeaks en su canal privado #command. Estaban furiosos con PayPal, pero, más que eso, vieron una oportunidad. La victimización de WikiLeaks, pensaron, tocaría la fibra sensible de Anonymous y atraería a una multitud de usuarios a su nueva red. Era una publicidad genial.[91]

Pero esta explicación apenas si roza la superficie de lo que sucedió. AnonOps estaba en modo reposo, sin prácticamente partidarios fuera del equipo principal. Esta llamada “oportunidad” solo se manifestó una vez que el mando de AnonOps se vio *obligado* a considerar su implicación después de las acciones independientes que llevaron a cabo un puñado desconocido de Anons, abriendo de este modo las puertas a la llegada de otros miles.

Podría decirse que el empujón inicial que revitalizó al equipo que estaba detrás de la Operación Venganza, impulsándole hacia la Operación Vengar a Assange, se originó en un póster bastante expresivo. En él se cubría de alabanzas a Assange: «Julian Assange diviniza todo aquello que

más valoramos. Él desprecia y lucha constantemente contra la censura [y] es probablemente el trol más exitoso de todos los tiempos... Ahora Julian es el objetivo principal de una caza mundial del hombre, tanto en el mundo físico como virtual.» Terminaba haciendo un llamamiento a Anonymous para que «devolviese el golpe por Julian» a través de la participación en múltiples actos políticos, desde ataques DDoS a PayPal hasta quejarse «a su diputado local».

El 4 de diciembre, mientras este mensaje circulaba por Internet, un grupo desconocido lanzó un ataque DDoS contra el blog de PayPal, muy probablemente mediante una botnet.[92] A esta acción le siguió un goteo de cobertura periodística y una declaración en el blog de seguridad PandaLabs que anunciaba, como un hecho objetivo, la implicación de AnonOps: «Los organizadores del grupo anónimo responsable de la Operación Venganza están reorientando su campaña para ayudar a WikiLeaks en su búsqueda por revelar documentos clasificados del gobierno.»[93] Ésta era la primera noticia para muchos en Anonymous. A medida que los informes de los medios de comunicación continuaban extendiéndose, en la sala de chat de #command de AnonOps estalló una discusión airada y farragosa. La mayor parte del equipo no tenía ni idea de que estuviesen «reorientando sus esfuerzos hacia WikiLeaks».

Para entender este momento podría servir de ayuda seguir a unos cuantos miembros de Anonymous (todos los seudónimos han sido cambiados) a través de los acontecimientos que se desarrollaron el 6 de diciembre. Comenzaron con Fred, uno de los participantes más importantes en #command (según uno de los entrevistados, «[Fred] es AnonOps»). Fred dedicaba un tiempo considerable al mantenimiento de la infraestructura. Una frase de Kurt Vonnegut me viene a la mente: «Otro fallo en el carácter humano es que todos quieren construir y nadie quiere encargarse del mantenimiento.» Fred estaba dispuesto a hacer el trabajo que los demás daban por sentado y, en consecuencia, estaba profundamente implicado en AnonOps. Aquel día, como explicó Fred en #command, estaba muy enfadado. En la hora que había de seguir tendría lugar una conversación que cambiaría para siempre el futuro tanto de AnonOps (específicamente) como de Anonymous (en general):

<Fred>: offs [oh me cago en la puta]

<Fred>: esa operación assange es solo un póster
<Fred>: ningún nombre de sitio, nada
<Fred>: no es nuestro

Trogo (autor del post en el blog PandaLabs) estaba en el canal. Era uno de un puñado de outsiders integrados a los que habían permitido el acceso a las áreas secretas —habitualmente eran muy pocos— con el fin de que seleccionaran información de los búnkeres de AnonOps y la volcaran al ámbito público. (Aunque Trogo es único en este sentido porque ha estado cerca de #command desde su creación.) Aparentemente, una declaración publicada por Trogo había impulsado a muchos a cometer acciones que ahora estaban siendo revisadas. Trogo defendió su precipitada decisión de publicar sin contar con un amplio consenso previo.

<Trogo>: [Fue] aprobado por Radwaddie [otro miembro de #command]
<Trogo>: Utilizamos el nombre porque los medios tienen una capacidad de atención muy corta
<Trogo> [a captor]: Anoche escribí un post en el blog anunciando el cambio de planes
<captor> [a trogo]: ¿qué cambio de planes?

Un cambio de planes había sido decidido efectivamente por aquellos que chateaban en AnonOps, pero la mayoría de Anons, incluso los que participaban en #command, no habían sido invitados a participar en el proceso de toma de decisiones. Cuando esta situación se volvió cada vez más evidente para los que habían quedado excluidos, muchos expresaron su inquietud y confusión. «Parece que aquí hay muchos que no lo saben», escribió Fred. A medida que la culpa circulaba, otros, estupefactos, se defendían: «no somos nosotros, no estamos disparando contra PayPal.»

A pesar de ser un outsider, Trogo procedió a recordar a los Anons cómo trabaja Anonymous: el nombre es libre para que lo tome quien así lo desee. Alguien señaló la ironía que suponía plantearle *a Anonymous* este hecho ostensiblemente conocido (y en lo que tal vez era el canal de IRC más importante de Anonymus en aquel momento, nada menos). Y además de establecer una obviedad, el bloguero e investigador de seguridad se defendió caracterizando lo que había ocurrido como de “nada nuevo”. Era perfectamente consciente de que el canal ya había decidido en gran medida

brindar su apoyo a WikiLeaks, aun cuando su compromiso de reflejar el sitio mediante la duplicación de su contenido todavía no se había actualizado. Reconociendo que no tenía sentido llorar por la leche derramada, Radwaddie pasó de la postura defensiva a la ofensiva, realizando un decidido intento de convencer a las partes descontentas para que aprovecharan el impulso y avanzaran, atacando a PayPal independientemente de la estrategia que ya se había elegido:

<Radwaddie>: ya que todos estamos de acuerdo en eso [ayudar a WikiLeaks]
<Radwaddie>: ¿por qué no estamos atacando a paypal?
<Fred>: ¿porque nadie sabía que se suponía que debíamos hacerlo?
<Radwaddie>: quiero decir, la mierda golpeando el ventilador ya, podría ayudarles también

Fue un movimiento astuto y oportunista y, casi de inmediato, el consenso comenzó a favorecer la postura de salir a la palestra. Pero había llamamientos al procedimiento debido. Si querían hacer las cosas correctamente era necesario que primero acelerasen su maquinaria propagandística. Mientras se influía sobre algunos para que favorecieran los ataques DDoS contra PayPal, la creciente ira (particularmente dirigida contra Radwaddie y Trogo por vulnerar el protocolo de la toma de decisiones) seguía extendiéndose a otros:

<dubiosdudious> [a Radwaddie]: ¿quién eres tú para tomar todas las decisiones?
<Radwaddie> [a dubiosdudious]: quieres sentarte y tomar una taza de té y discutir la siguiente causa de la acción?
[...]
<Radwaddie> [a dubiosdudious]: ¿cuál es tu objeción? (punto por favor)
<dubiosdudious>: 1. sin preparativos
<dubiosdudious>: 2. sin votación
<dubiosdudious>: así a bote pronto

Mientras Radwaddie intentaba impulsar la campaña a pesar de los ataques que estaba recibiendo, comenzaron a entablarse discusiones semánticas sobre el papel que cumplía #command en general. Radwaddie gritó-tecleó: «de acuerdo, joder, ¿QUIÉN COÑO TIENE ALGUNA IDEA AQUÍ?» Y mientras la semilla germinaba entre los Anons reunidos, el debate lentamente —tal vez inexorablemente— pasó de la cuestión de *si* se debía

atacar a PayPal, a la cuestión de *dónde* atacar a PayPal. La mayoría de los participantes eran partidarios de hacerlo en el "sitio principal". Entonces Radwaddie combinó los argumentos morales y pragmáticos: «estamos tratando de plantear una cuestión, [que] estamos en desacuerdo con paypal [que es la razón por la que] hacemos lo que mejor sabemos hacer: ddos.» Escribió que Anonymous trataba de eso, no de «discursos impresionantes o de una comunidad fabulosa». Justo cuando el apoyo a la posición de Radwaddie parecía alcanzar un consenso, alguien llamado "lark" entró en la sala de chat con una información sorprendente: «el ataque [inicial] contra el blog de paypal lo lanzó uno de los nuestros como un proyecto paralelo.» De modo que, de hecho, el primer ataque DDoS, que todo el mundo pensó que había sido instigado por un Anon no afiliado, había sido ejecutado por uno de los suyos. Supongo que él simplemente había seguido su camino sin hacer ruido, ya que en aquella época AnonOps estaba centrado fundamentalmente en apoyar el intercambio de archivos.

Pero a pesar de esta revelación, parecía que el impulso ya no podía detenerse. Teniendo en cuenta el alboroto generado por la decisión de Trogo y Radwaddie de aprovechar el primer ataque DDoS, que todo el mundo pensó que era obra de un outsider, podría parecer inverosímil que nadie respondiera a lark. Pero podemos imaginar que, llegados a este punto, los Anons estaban tan profundamente inmersos en su curso de acción —debatiendo objetivos y estrategia— que esta declaración les resultó fácil de ignorar. La conversación, simplemente, continuó. Finalmente, se hizo un anuncio:

> <captor>: HECHO
> <captor>: tenemos un objetivo [el sitio principal de paypal]

Se comunicó la decisión al equipo de propaganda y se inició el ataque (con botnets que habían sido desplegadas en secreto). La conversación pasó naturalmente a considerar la importancia de ampliar el alcance de la Operación Venganza (conocida también como "o:p") para incluir otros asuntos aparte de los derechos de autor y la piratería:

> <Mobile>: ¿de modo que o:p se ha convertido en una guerra sobre la censura y los derechos de autor?
> <Radwaddie>: y lo consideramos como una operación paralela, no estamos

suspendiendo nuestras actividades “normales” [...]
<Trogo>: ¿Es siquiera posible atacar con un DDoS a PayPal?
<Radwaddie> [a Trogo]: lo averiguaremos, ¿verdad?

El ataque, ignorado por todos los participantes, ya no era solo una “operación paralela” iniciada por los Anons en #command. Se trataba, en cambio, de la salva de apertura que daría lugar a un movimiento mundial, abriendo la puerta a una nueva era de Anonymous. Este nuevo nodo tendría miles de participantes y no sería el producto de una determinación obvia y directa, sino más bien de la confusión: una mezcla de manipulación, información falsa, buenas intenciones e incertidumbre generalizada.

No lo buscaron, no lo eligieron

La respuesta a la pregunta de Trogo —«¿Es siquiera posible atacar con un DDoS a PayPal?»— resultó ser «sí». (También resultó ser cierto en el caso de MasterCard y de muchas sociedades financieras.) Lo que se había concebido como una simple diversión se metamorfoseó con bastante rapidez en una apoteosis de AnonOps. Entre el 6 y el 8 de diciembre de 2010, AnonOps extendió su radio de acción colocando en su punto de mira no solo el blog y el sitio web de PayPal, sino también los sitios web del fiscal sueco (ya que el gobierno sueco intentaba extraditar a Assange, acusado de violación)[94] y los del senador Joe Leiberman, Sarah Palin, MasterCard, Visa, EveryDNS (un proveedor de servicios de nombres de dominios) y otros. Exigiendo venganza contra cualquier parte cómplice en la difamación de WikiLeaks, AnonOps provocó que todos estos sitios sufrieran cierto periodo de inactividad, aunque las horas exactas varían dependiendo de la persona a la que le preguntes. El 8 de diciembre, los números en el canal principal #operationpayback en IRC alcanzaron la cifra inusitada de 7.800.

Estos ejemplos demuestran cómo las tácticas empleadas por Anonymous se ajustan al relato de Michel de Certeau cuando se refiere a «tácticas de resistencia cotidianas» por las cuales «una táctica depende del momento, está siempre a la expectativa de las oportunidades que deben aprovecharse ‘al vuelo.’»[95] Radwaddie y Trogo decidieron actuar

independientemente del grupo, aprovechando exactamente esta clase de ocasión tan oportuna; este estilo de toma de decisiones sobre la marcha es un elemento básico de Anonymous. A menudo, el grupo se muestra más reactivo que proactivo; parafraseando el poema que sirve de introducción a este capítulo: *la decisión les fue impuesta, no podían rechazarla, ellos no la buscaron, ellos no la eligieron, pero dependía de ellos*. Sin embargo, para ejecutar plenamente la operación se requerían una considerable organización y recursos, que en este caso asumieron la forma de botnes zombis y voluntarias y propaganda.

El factor que marcó la diferencia era a la vez simple y escapaba simplemente al control de Anonymous: fue la indignación general con respecto al bloqueo del pago. Internet estaba inundada de artículos y tuits que expresaban inquietud; todo el mundo hacía su propia versión de la pregunta formulada por un periodista británico en Twitter: «¿De qué han sido declarados culpables realmente Assange o Wiki-leaks [*sic*], que permita a VISA, Mastercard, PayPal y Amazon retirar el servicio esta semana?»[96] Para ilustrar la hipocresía que rodeaba a todo este asunto, la gente señaló que mientras MasterCard se negaba a procesar los pagos a WikiLeaks, los racistas de todo el mundo tenían libertad para hacer donaciones a la organización racista de su elección, como el Ku Klux Klan. El experto en Internet Zeynep Tufekci publicó la siguiente advertencia:

> El furor desatado por WikiLeaks nos demuestra que estas instituciones de poder están tomando el control, de forma lenta pero segura, de los momentos críticos de Internet. Como una simple “esfera cuasi pública”, Internet se parece en cierto modo a los centros comerciales, que son como espacios públicos pero donde los derechos de los ciudadanos están restringidos, ya que, de hecho, son privados.[97]

No había duda de que todo el mundo afrontaba esta cruda realidad: Internet, vivida tan a menudo como un espacio público es, de hecho, una zona privatizada, con los Amazons y PayPals del mundo capaces de cerrar las conversaciones y el comercio.

El ánimo que reinaba en determinados círculos en aquella época quedó reflejado en la siguiente declaración de un activista que participaba en Twitter bajo el nombre de “AnonyOps” (sin relación alguna con AnonOps,

si bien los nombres guardan un parecido evidente):

> Recuerdo que se estaba creando una montaña de angustia y hasta ese día no me di cuenta de que no era una montaña. Era un volcán, y el día que se suspendieron las donaciones a WikiLeaks, el volcán estalló y ese fue el día en que busqué una manera de llamar la atención sobre toda esa mierda. Una manera de hablar públicamente sin poner en peligro mi carrera.[98]

Un ingeniero cualificado y rico que rondaba la treintena creó la cuenta de Twitter AnonyOps (con el tiempo se convertiría en una de las mayores cuentas de autor múltiple de Anonymous) y, como muchas otras, la cargó en el IRC.

AnonOps, porque no era una gota amorfa sino más bien un equipo con recursos y con una fuerza de voluntarios entregados, había creado una plataforma desde la cual podía actuar toda clase de personas. La confusión y la casualidad se mezclaban con la disponibilidad operativa y el despliegue de recursos. Manadas de ciudadanos preocupados de todo el mundo se sumaban a aquel ejército contestatario.

«Buenas noches y dulces sueños de parte de AnonOps»

En otoño de 2010, cuando AnonOps estaba lanzando una oleada tras otra de ataques DDoS en el marco de la Operación Venganza, yo me había tomado un permiso para ausentarme de Anonymous con el propósito de acabar mi primer libro sobre piratería de software libre. El libro llevaba retraso y, como el reloj de mi plaza en la universidad avanzaba implacablemente, la presión era muy fuerte. Me agobiaba psicológicamente: para conservar mi trabajo tenía que publicar un libro. De modo que me reservé el mes de diciembre para esprintar hasta la línea de meta. Cuando a principios de diciembre Anonymous resurgió como una fuerza activista, confié en mi capacidad de Mujer Araña: me parecía demasiado importante históricamente como para ignorarlo. Dejé a un lado el manuscrito y concentré toda mi atención en Anonymous. Para ser totalmente honesta, la apuesta parecía segura; haciendo una extrapolación de acciones pasadas,

pensé que este nuevo fenómeno podía agotarse, o al menos ralentizarse, transcurrido un mes y entonces podría regresar a trabajar en mi libro. Pero, en lugar de eso, permanecí encadenada al ordenador durante casi tres años.

Aquel diciembre, en plenas vacaciones, viajé a la costa oeste a pasar algún tiempo con mi familia. Mientras mis familiares disfrutaban de los placeres del senderismo por los escarpados acantilados sobre el brillante océano Pacífico y miraban películas hasta bien entrada la noche, yo permanecía acurrucada junto a mi portátil. Estaba absorta, perpleja y colgada de la energía y excitación salvajes que viajaban por los canales. Estoy bastante segura de que mi familia pensaba que mi comportamiento antisocial era deliberado, y no le faltaban razones para ello. Yo era sin duda la huraña del grupo, nunca tan ilusionada como todos los demás por el ambiente navideño, el ponche de huevo ni (muy especialmente) por los juegos de mesa que a ellos tanto les gustaban y yo tanto odiaba. En cualquier año tenía media docena de excusas en la punta de la lengua ante la mera sugerencia de jugar a *Los colonos de Catán*.

Para gran parte de mi familia, Internet representa la temida tarea del correo electrónico; para ellos es el lugar donde leen las noticias matutinas mientras toman café, examinan Facebook en busca de las últimas fotografías de sus amigos y sus angelicales bebés y, en momentos de desesperación en el lugar de trabajo, disparan fantásticos vídeos de gatitos. Internet es todas esas cosas también para mí, pero es algo más, un lugar de mundos múltiples; una galaxia, de hecho. Para ellos, sencillamente, no es un "lugar" donde algo como las protestas contra la Organización Mundial del Comercio, que se llevaron a cabo por sorpresa en Seattle hace más de diez años, pudiera llegar a ocurrir. Y, sin duda, hay un abismo entre los gases lacrimógenos y el acto de aporrear un teclado. Pero, inconmensurabilidades aparte, una cosa era segura: yo estaba asistiendo a la primera protesta popular, concentrada y a gran escala en la red y no pensaba perdérmela por nada del mundo, especialmente *no* por *Los colonos de Catán*.

Después de una larga jornada de investigación no deseaba otra cosa que describirle a mi familia las apasionadas y bulliciosas escenas que había visto en la pantalla. Pero me costaba encontrar las palabras y la terminología adecuadas. Durante semanas había luchado por familiarizarme con las cosas y poder juzgar qué clase de "manifestación masiva" se estaba

llevando a cabo. Me vinieron a la cabeza preguntas en lugar de respuestas: ¿era desobediencia civil? ¿Acción directa? ¿Algo parecido a una manifestación callejera? ¿Una sentada virtual? ¿Un bloqueo? ¿Violaban los ataques DDoS la libertad de expresión y algunas libertades fundamentales, como afirmaban algunos críticos? ¿Era algo ético, poco ético, eficaz, ineficaz? ¿Quién era toda esa gente, al fin y al cabo?

Al principio solo tenía una vaga idea. Había tantos apodos zumbando junto a mí en el IRC..., pronto estaría chateando sin cesar con varios de ellos y, finalmente, llegaría a conocer a un pequeño grupo en persona. Pero en aquel momento eran un misterio para mí. No sabía nada de la existencia de canales extraoficiales secretos; estaba concentrada principalmente en las conversaciones que se desarrollaban en #operationpayback y otros canales públicos. También tuve que aprender cómo funcionaba LOIC a nivel técnico y tuve que volver a leer las campañas de DDoS que AnonOps había llevado a cabo en otoño. La velocidad y el mero número de participantes hicieron que todas las conversaciones anteriores que había presenciado en el IRC parecieran triviales. Aunque estaba invirtiendo muy poca energía física —sentada todo el día, mirando fijamente las conversaciones en la pantalla del ordenador—, al acabar el día me dolía la cabeza. Estaba agotada y tenía la opinión dividida sobre todo aquello. Me llevó varias semanas procesar la ética implícita en la manera como Anonymous dirigía sus campañas de DDoS.

La cantidad de información procesada requerida de los participantes era asombrosa. Al conectarte al canal principal aparecía una pantalla que mostraba el tema y una breve sinopsis de la información sobre el objetivo elegido: la dirección de IP para acceder a LOIC, canales de Twitter que debías consultar para tener contexto y otros canales de IRC que merecía la pena visitar. Habitualmente, el aspecto era algo parecido a esto:

> (04:56:18 PM) El tema para #opb es: OPERACIÓN VENGANZA “http://anonops.eu/”http://anonops.eu/ | Twitter:“http://twitter.com/Op_anon ”http://twitter.com/Op_anon |
> “http://www.justiceforassange.com/”http://www.justiceforassange. com/Hive: 91.121.92.84 | Objetivo: “http://www.mastercard.com/”www.mastercard.com | Ver: #Setup #Target #WikiLeaks #Propaganda #RadioPayback #Protest #Lounge y /lista para el resto | “http://808chan.org/tpb”http://808chan.org/tpb

Anonymous estaba reproduciendo, conjuntamente, un montón de manifiestos, vídeos y pósters bien argumentados; Anonymous había explotado un desencanto profundo y extendido y, mediante la aportación de una vía para el activismo agresivo, lo había canalizado hacia una forma más coherente y visible. Era como si todos supieran que estaban asistiendo a un momento histórico: la primera sublevación popular en Internet. Completos desconocidos se comunicaban para trabajar en un objetivo común. Yo misma me sentía inspirada.

Las conversaciones eran un asunto completamente distinto. Con miles de personas conectadas y un centenar de usuarios hablando a la vez, era algo extremadamente cacofónico y exigía hasta la última pizca de mi cerebro, ya de por sí afectado por el TDAH (Trastorno por Déficit de Atención con Hiperactividad) para poder seguir el hilo. De hecho, probablemente no existe en el mundo ningún otro medio tan favorable a lo que el teórico literario Mikhail Bakhtin denomina "polifonía" (una multiplicidad de voces, cada una con una perspectiva y un peso moral únicos) como el IRC.[99] Y si bien algunos describirían a Anonymous como «un microcosmos de anarquía, sin moral, empatía o agenda»,[100] yo observé algo completamente diferente: todos tenían un punto de vista ético, una razón para estar allí. Estaban preocupados, querían hacer justicia, querían acabar con la censura (y algunos incluso estaban allí para discrepar —con vehemencia— de las tácticas empleadas). Cierto: como colectivo, Anonymous no tenía un mandato universal, pero sus participantes tenían sus propias brújulas morales, a menudo bien ajustadas, para orientarse.

Para tomar un solo ejemplo de entre las docenas de temas que se debatían acaloradamente: en diciembre de 2010, #operationpayback alojó un estruendoso debate sobre la eficacia y la ética de la protesta tecnológica en general y del DDoSeo en particular. Había dos subtemas que destacaban por encima de los demás: la seguridad de LOIC y la cuestión más filosófica de si el DDoSeo es un ejercicio del derecho a la libre expresión o un acto destinado a impedir que los demás ejerzan ese derecho. Los extractos tomados de dos conversaciones diferentes, incluidos a continuación, ejemplifican el carácter polifónico de estos intercambios y la multiplicidad de posturas éticas en estas protestas tecnológicas. Estas cuestiones fueron visitadas y revisitadas a lo largo del mes.

A comienzos de la campaña, los participantes hicieron frente a la

trascendencia política de Anonymous, casi todos expresando su apoyo al DDoS:

<P>: esto es mejor que OMC Seattle
[...]
<P>: enfoque ascendente
<z>: sin embargo necesitas una masa crítica antes de que la gente comience a sentirse inspirada
<z>: 2 o 3 personas participando no parece algo épico, parece más bien débil
<a>: este ataque parece bastante desorganizado en este momento
<z>: tiene que hacerse viral, ¿sabes?
<P>: un mensaje bastante atractivo en mi opinión
[...]
<a>: creo que estos ataques no tratan tanto de hacer daño a las empresas como de atraer la atención y obligar a que los medios cubran la historia
<a>: la mayoría de las personas que conozco ni siquiera han oído hablar de WikiLeaks hasta que saco el tema
[...]
<a>: Mi opinión es que esta es la vía tecnológica de protesta masiva que resulta realmente eficaz, de modo que hasta que no exista libertad de información total no habrá un final.
[...]
<m>: no hay nada malo con la protesta tecnológica. es solo que luchamos para organizarnos. no hacemos ningún daño. casi ninguno de nosotros es un hacker propiamente dicho.
<P>: twitter sincronizado y posteo en facebook, banderas piratas en Internet cada vez que puedas y luego un manifiesto sobre cómo llegar a la esquina de tu calle local y hacer algo
[...]
<P>: anon puede poner esto en movimiento pero se trata de algo más grande que anon

Pocos días más tarde, en el mismo canal, después de algunos DDoSeos, mientras otros seguían defendiendo esta línea de acción:

<26>: no creo que DDoS pueda hacerse en nombre de la libertad de expresión
<26>: porque se trata de un acto de silenciamiento
<matty>: ^
<sc>: piensa en un objetivo como un cartel en un edificio
<secreta>: está bastante claro cuán hipócrita me parece el ddos

> <PN>: sigues gritando que todo el mundo irá a la cárcel. Solo estás aquí para desanimar al personal. zorra.
> <sc>: no estás de acuerdo con lo que representa ese edificio
> <26>: pero la gente irá a la cárcel
> <ri>: NO TENGAS MIEDO DE LA CÁRCEL
> [...]
> <ri>: toda protesta por los derechos civiles acaba con gente en la cárcel

Para la gran mayoría de los participantes que contribuyeron a utilizar o utilizaron la LOIC, se puede asumir que consideraban tanto la herramienta como la táctica un método de protesta moralmente aceptable. Otro tema era si la LOIC era en efecto una herramienta *legal*. En aquel momento la línea partidista de AnonOps afirmaba que DDoSear con LOIC era una acción segura: no porque la herramienta convirtiese en anónima tu dirección de IP (no lo hacía y, en general, nadie declaró que lo hiciera), sino porque la enorme cantidad de personas que participaba en la acción haría que fuese prácticamente imposible o, al menos, excesivamente incómodo, que las autoridades pudieran localizar y arrestarles a todos. Los principales operadores en el canal #operación-venganza, algunos de los cuales también participaban en el canal #command, excluyeron, en algunos momentos, a aquellos que advertían a otros sobre su carácter ilegal. Quienes estaban en #command querían infundir confianza en sus métodos, no miedo. AnonOps también hizo circular "instrucciones" sobre la manera de utilizar la LOIC, que incluía un consejo espantoso de seguridad acompañado del abiertamente agresivo —y en extremo dudoso— consejo legal en caso de ser arrestado:

> SI TE V& [enjaulan] debes declarar que no tuviste ninguna participación en este acto. Menciona que estás utilizando una dirección de IP dinámica y que muchas personas la utilizan porque es dinámica. Si demuestran que era tuya, entonces debes decirles que eres víctima de un "virus botnet" del que no tenías control ni conocimiento. Además, si colocas tu dispositivo inalámbrico en modo no garantizado o WAP (protocolo de aplicaciones inalámbricas) antes de utilizar la herramienta LOIC puedes alegar que alguien hackeó tu dispositivo inalámbrico. Caso cerrado.[101]

Más escandaloso aún fue el hecho de que una pequeña cohorte de periodistas difundió información errónea. Si tal vez a Anonymous se le podía entender y perdonar por sus errores, los periodistas deberían haber hecho sus deberes en lugar de limitarse a reproducir los consejos legales erróneos y la información técnica engañosa suministrada por sus fuentes. El ejemplo más grave de esta práctica provino del popular sitio de noticias tecnológicas Gizmodo, el 8 de diciembre de 2010, en un artículo titulado "¿Qué es LOIC?": «Debido a que un DDoS lo desconecta prácticamente todo, al menos cuando funciona como está previsto, los archivos de registro que habitualmente registran cada conexión entrante simplemente no funcionan.»[102] Este punto es totalmente incorrecto. El sitio sometido a un ataque DDoS puede seguir controlando su tráfico, eliminando selectivamente y conservando direcciones de IP, que luego pueden ser utilizadas para identificar a los participantes.

La LOIC es tan segura como un condón roto. Si una persona que utilizaba la LOIC no tomaba medidas para proteger su dirección de IP, ésta se mostraba claramente en cada paquete —en cada ataque— trasmitido. Muchos participantes probablemente carecían del más rudimentario conocimiento sobre cómo funcionaba la tecnología, una necesidad básica para tomar una decisión fundada. El calor del momento y la sensación de seguridad dominante vencieron por igual a periodistas y participantes. En general, y con escasas excepciones, la mayoría de la gente implicada en #command, por muy ingenua que pudiera parecer su posición retrospectivamente, era sincera, creo yo, al creer que la protección se derivaba de la fuerza de los números. Algunas de las personas que participaron en #command utilizaron la herramienta LOIC y posteriormente fueron arrestadas.

Durante gran parte del otoño de 2010, Anons utilizó los ataques DDoS sin mayores repercusiones, potenciando un falso sentido de seguridad que muy pronto se desvanecería a consecuencia de los primeros allanamientos practicados por el FBI a finales de diciembre. También estaba la cuestión de los mensajes personalizados que acompañaban los ataques DDoS. Cuando las personas se conectaban a la colmena AnonOps, y se enviaban paquetes a un objetivo, se incluía un mensaje: «Buenas noches y dulces sueños de parte de AnonOps.» El gobierno seguramente podía utilizar este mensaje para neutralizar las alegaciones de que el remitente había sido, sin saberlo,

«víctima de un virus botnet». Pero, con el asesoramiento de un buen abogado, ese argumento se derrumbaba porque se podía identificar el mensaje como parte del virus (el problema es que los buenos abogados son caros). En cualquier caso, nada de esto fue analizado ni, aparentemente, entendido.

La situación cambió rápidamente. Poco después de la primera oleada de ataques, un póster advirtiendo que la LOIC era insegura recorrió la red. El mal consejo ofrecido por sitios como Gizmodo no tardó en ser rectificado por artículos cuidadosamente investigados en sitios como Boing Boing, proporcionando advertencias y detalles técnicos precisos relativos a las vulnerabilidades de seguridad de la LOIC. Aproximadamente en esta época, un talentoso programador consiguió reunir un pequeño grupo de Anons con el fin de comenzar a escribir una versión más segura, aunque más difícil de usar. Una vez publicada fue descargada masivamente antes de que la gente se diera cuenta de que contenía un troyano.

Finalmente llegó una prueba de rastreabilidad irrefutable: agentes de la ley vistiendo chaquetas azules con las letras FBI impresas en amarillo visitaron alrededor de cuarenta hogares repartidos por Estados Unidos, incautándose de discos duros cargados con datos incriminatorios. Finalmente, en julio de 2011, el FBI arrestó a catorce presuntos participantes, trece de los cuales han sido declarados culpables. En octubre de 2013, un gran jurado acusó a trece ciudadanos estadounidenses de haber participado en la Operación Vengar a Assange y en algunos de los primeros ataques de la Operación Venganza.[103]

Ahora todo el mundo sabía que la LOIC era una herramienta insegura, que el gobierno de Estados Unidos estaba dispuesto a perseguir a los manifestantes políticos online, incluso a aquellos que no habían utilizado la LOIC (algunos de los participantes arrastrados por el operativo DDoS nunca utilizaron la LOIC ni botnets, pero fueron acusados sobre la base de las conversaciones registradas en IRC); y no había ninguna seguridad en los números. Presumiblemente se había aprendido una dura lección.

El DDoS como contorsión moral

Equipados con estos detalles, ¿qué reflexiones éticas e históricas podrían

extraerse de estos extraordinarios actos de acción directa, la mayor demostración política de DDoS que la web había experimentado? En otoño de 2010, el empleo de ataques DDoS era una táctica política establecida entre los hacktivistas; Anonymous no fue en absoluto el precursor de esta técnica. En la década de 1990 y principios de los años 2000, el Electronic Disturbance Theater (EDT) (Teatro de la Perturbación Electrónica), por ejemplo, montó una serie de campañas DDoS que denominó “sentadas virtuales”. Estas acciones combinaban las intervenciones técnicas con poesía y performance. El EDT se centró en los sitios web del gobierno mexicano para divulgar la difícil situación que estaban viviendo los zapatistas que luchaban por conseguir la autonomía de la región de Chiapas, México.[104] Repartían notas de prensa antes de los actos y, aunque no conseguían reunir a más de un centenar de participantes y no provocaban ninguna inactividad en los sitios web, alcanzaron (de alguna manera) su objetivo de concitar la atención de los medios de comunicación. En cualquier caso, la acción difícilmente podía calificarse, tal como ha señalado acertadamente Molly Sauter, de “desestabilizadora”[105] y en ningún momento alcanzó un punto de saturación en los principales medios de comunicación.

Anonymous alteró lo bastante la escala, la expresión y los efectos del DDoSeo como para que el grupo rompiera el molde que había heredado. En lugar de dedicar meses a organizar actos pequeños y bien elaborados, Anonymous experimentó con el arte de convertir la ira en tiempo real en una rebelión salvaje, imprevisible y permanente. Como sucede con cualquier manifestación asamblearia pública, junto a los políticamente motivados estaban aquellos que solo eran compañeros de viaje y aquellos que estaban allí simplemente para lograr que el viaje fuese lo más accidentado y salvaje posible. Resulta inevitable que los participantes en Anonymous tengan una amplia variedad de posturas y resultados deseados, teniendo en cuenta la base filosófica del grupo y la accesibilidad de sus herramientas de software. Las acciones están abiertas por igual a activistas veteranos y a recién llegados.

A la luz de una consideración histórica de esta táctica podemos ver claramente que el DDoSeo no es nada nuevo, ya que virtualmente todo movimiento que haya defendido el cambio social en los últimos doscientos años (desde los abolicionistas hasta ACT UP, acrónimo de *AIDS Coalition*

to Unleash Power, “Coalición del SIDA para desatar el poder”) se ha basado en el empleo de tácticas a gran escala, ruidosas y desestabilizadoras, para llamar la atención y exigir el cambio.[106] La novedad reside en la manera en que la disponibilidad de una herramienta de software, la LOIC, y la plataforma publicitaria de Anonymous que divulgó su existencia, permitieron que unas manifestaciones tan considerables y molestas echaran raíces y se desplegaran casi espontáneamente en Internet. En un detallado análisis de las características de la herramienta, Sauter afirma de forma convincente que el “modo Mente de Colmena” contribuyó a asegurar esos números considerables: «Aunque Anons tal vez no ‘salió a las calles’ como había imaginado el EDT, el modo Mente de Colmena sí les permitía ir a la escuela, trabajar, dormir o ir a cualquier parte mientras seguían participando en acciones DDoS a medida que surgían.»[107]

Pero aunque el DDoS se limite a continuar una extendida tradición de activismo agitador es, no obstante, una propuesta que entra en conflicto con muchos Anons y hackers, incluso entre aquellos que no tienen ningún problema con infringir la ley. Un día, mientras chateaba con un hacker de Anonymous sobre el carácter moral de las protestas, me dijo: «Intentar encontrar una defensa ética segura para el DDoSeo de Anonymous sólo conseguirá meterte en una contorsión moral.» Para muchos Anons resultó especialmente problemático descubrir que las campañas de DDoS realizadas en el otoño y el invierno de 2010, incluida la Operación Vengar a Assange, se basaban en el engaño y estaban reguladas mediante el despliegue de botnets controladas por hackers. Si los participantes hubiesen sabido que era un ejército de ordenadores zombies quien proporcionaba la munición, quizá su elección habría sido diferente.

Y, no obstante, sin el impulso de aceleración facilitado por esta red de ordenadores secuestrados, el uso de la LOIC —incluso por miles de participantes dispuestos y comprometidos ideológicamente, cada uno de los cuales aportaba una pizca de potencia— nunca hubiese provocado las desactivaciones que generaron la ansiada atención de los medios de comunicación. Este mismo hacker, crítico de la técnica, se extendió en su análisis: «He mantenido numerosas discusiones sobre el DDoS con personas que, igual que yo, no son abiertamente partidarias de esa herramienta, pero volvemos una y otra vez a ella porque es eficaz; los medios de comunicación impulsan gran parte de esta actividad.»

Fue fundamental. Una participación pública sólida puede no haber sido técnicamente necesaria, y las afirmaciones acerca de la seguridad de la LOIC estaban radicalmente equivocadas, pero sin la aparición de una masa crítica es probable que la operación hubiese carecido de autoridad y dignidad moral. En este caso, la fuerza de los números transmitió un potente mensaje, aun cuando en ellos no hubiera ninguna seguridad (ni ninguna necesidad técnica): reveló de manera palpable al mundo en general hasta qué punto sus partidarios estaban desencantados ante lo que consideraban una muestra de censura corporativa.

Geeks y otro tipo de personajes también formularon críticas más generales contra esta táctica, luchando por establecer una analogía entre la campaña de DDoS y equivalentes offline. Más persistente era la idea de que los ataques DDoS pisoteaban el derecho a hablar libremente de los objetivos atacados. Si uno adopta una visión absolutista de la libertad de expresión, entonces el DDoS anula la posibilidad de expresión mediante la desactivación del acceso a un sitio web que expresa un conjunto de ideas. Esto refleja la postura de algunos hackers, como Oxblood Ruffin, del Culto de la vaca muerta, absolutamente contrarios a esta táctica desde hace décadas. En el transcurso de una entrevista con CNET, Oxblood Ruffin razonaba de la siguiente manera: «Anonymous lucha por la libertad de expresión en Internet, pero es una postura difícil de apoyar cuando estás practicando el DDoSeo y no permites que la gente hable. ¿Qué coherencia tiene eso?»[108]

Tiene razón hasta cierto punto. Una concepción más dinámica de la libertad de expresión podría tener en cuenta las relaciones de poder. Al permitir que el desvalido —el manifestante o grupo vulnerado— se exprese con una voz tan alta como la de sus oponentes más ingeniosos (en este caso, corporaciones poderosas), podríamos entender una táctica como el DDoS como un elemento nivelador: un triunfo de la libertad de expresión. Soy partidaria de un análisis de la libertad de expresión más contextualizado e impulsado por el poder. En el caso de Vengar a Assange, PayPal y los de su clase nunca perdieron realmente la capacidad de hablar y la propia acción se produjo en respuesta a un bloqueo bancario y de servicio unilateral que anuló la capacidad de WikiLeaks de hablar o exponer una postura. Mientras que WikiLeaks disponía de un único punto de salida proactivo —su sitio web desactivado (y el ocasional periodista comprensivo)— muchos de los

objetivos, como el MPAA y PayPal, controlaban a grupos de presión, anunciantes y contactos en los medios de comunicación capaces de distribuir su mensaje a los cuatro puntos cardinales.

Pero concebir el DDoS como un elemento modulador de la libertad de expresión es polémico en sí mismo. Otros piensan que se alinea mejor con otra táctica de protesta tradicional: el bloqueo de la acción directa. En un debate entre miembros del Culto de la vaca muerta, el hacker Tod Gemuese hizo la analogía de la libertad de expresión con "tonterías." Y añadió: «Es el equivalente digital de formas de protesta en el mundo físico como cerrar con candados el portón de una fábrica u obstruir el acceso a un edificio, etcétera.»[109] Aquellos que se mostraban críticos con esta táctica porque las empresas tenían que dedicar recursos a proteger sus sitios web no entendían la naturaleza de la acción directa. La acción directa supera una política liberal de publicidad, discurso y debate, con el objetivo de detener directamente la actividad o afectar y causar inconvenientes a la parte objeto del ataque.[110] El DDoS satisface esos requisitos.

Todos estos argumentos, por supuesto, no justifican necesariamente el DDoS en todas las situaciones. En cambio demuestran de una manera más detallada su lógica de la contorsión y su relacionalidad ética. El estudioso de Internet Ethan Zuckerman y sus colaboradores han escrito de manera convincente sobre cómo el DDoS puede llegar a perjudicar a las organizaciones pequeñas que carecen de los recursos defensivos de una corporación importante.[111] Incluso si uno apoya su uso restringido (digamos, contra organizaciones poderosas y que cuentan con grandes recursos), la proliferación de DDoS, acusan los críticos, continúa promoviendo el uso de una táctica que puede degenerar rápidamente en una carrera armamentística donde aquellos que cuentan con un mayor ancho de banda pueden superar a quienes lo tienen menor.

Más allá de lo que pudiera pensarse sobre la utilidad y la moral de la táctica, podemos ampliar nuestra perspectiva si tenemos en cuenta el verdadero resultado técnico y jurídico de un ataque DDoS típico. Esto nos ayudará también a sopesar la equidad (o la falta de ella) de los castigos aplicados a los participantes. A pesar de los informes erróneos divulgados por los medios de comunicación, los servidores que soportan el tráfico de DDoS no son hackeados y tampoco sufren ningún daño ni pérdida de datos permanente.[112] Los costes en los que se incurre son consecuencia

principalmente de que los objetivos necesitan contratar a empresas que les proporcionen protección contra los ataques DDoS. Un ataque DDoS hecho con éxito contra una empresa determinada bloquea el acceso a un dominio de Internet. Esto puede paralizar el acceso al comercio electrónico, pero no afecta al sistema informático interno de la organización. Los ataques típicos de DDoS, o “flujos de tráfico”, perpetrados por Anonymous resultaban infructuosos contra sitios de servicio que llevan a cabo una gran cantidad de transacciones de datos y cubiertos por Redes de Entrega de Contenidos (CDN), como Amazon.com (AnonOps intentó atacar directamente a Amazon.com y fue un fracaso estrepitoso). Incluso con los miles de personas que aportaban sus ordenadores a una botnet voluntaria, sus esfuerzos nunca consiguieron bloquear pilares infraestructurales como Amazon Web Services. Las campañas de DDoS llevadas a cabo por Anonymous salían mejor cuando los objetivos eran sitios internacionales como mpaa.org. Las tácticas de protesta digital de Anonymous bloqueaban básicamente el acceso a estos dominios, pero solo sus sitios web conectados a Internet.

Teniendo en cuenta lo que sucede durante un ataque DDoS, e independientemente de lo que se pueda pensar de sus riesgos y de su seriedad, una cosa parece segura: los cargos presentados contra los participantes de Anonymous en Estados Unidos y el Reino Unido tienden a no coincidir con la naturaleza no violenta de estas acciones. En Estados Unidos, los arrestos por ataques DDoS se llevaron a cabo en el marco de la Ley de Abuso y Fraude Informático (CFAA), que tiende a acarrear penas más duras si las comparamos con los cargos presentados bajo estatutos análogos para delitos cometidos fuera de la red. Las tácticas de protesta fuera la red, como invadir la propiedad o el vandalismo —donde el daño no es meramente especulativo— raramente tienen consecuencias catastróficas para los participantes. Sin embargo, este matiz que reconoce la intención y las consecuencias de las acciones cometidas, raramente se concede a las actividades virtuales, especialmente cuando se invoca la CFAA. Como consecuencia de esta situación, una conducta similar que a un infractor podría costarle ser acusado de una infracción o un delito menor offline (con una pena de unos treinta días en prisión) se castiga como un delito grave cuando tiene lugar en la red, con una multa considerable y la condena a prisión.

Para que nos hagamos una idea: en el estado de Wisconsin, un transportista de 38 años, Eric J. Rosol, fue multado por ejecutar una herramienta DDoS automatizada contra el sitio web de Koch Industries durante sesenta segundos. (Como parte de una operación de Anonymous, Rosol estaba protestando por el apoyo de los multimillonarios hermanos Koch a la iniciativa del gobernador de Wisconsin de reducir el poder de los sindicatos y los derechos de los empleados públicos a participar en negociaciones colectivas.) Las pérdidas económicas reales fueron inferiores a los 5.000 dólares, pero Rosol fue multado con 183.000 dólares, aunque en el mismo Estado un delito físico mucho más grave como es el incendio provocado está sancionado con una multa de tan solo 6.400 dólares.[113] La multa equivale al coste que les supuso a los hermanos Koch contratar a una empresa de consultoría antes de la campaña para que les aconsejara sobre cómo mitigar el ataque. En el Reino Unido, Chris Weatherhead —quien no contribuyó directamente a una campaña DDoS pero dirigía el centro de comunicación de Anonymous donde se coordinaban las protestas— recibió una exagerada sentencia de dieciocho meses de prisión, «condenado por un cargo de conspiración para perjudicar el funcionamiento de ordenadores».[114]

Las consecuencias jurídicas para las personas arrestadas por los ataques a PayPal merecen un análisis más detallado. Debido a una excelente asistencia legal y a un trato negociado (aún en ciernes), la mayoría de los trece acusados de haber realizado un ataque DDoS contra PayPal recibirá una multa de solo 5.600 dólares cada uno y no deberán ingresar en prisión. Aunque serán acusados de delitos mayores, es probable que el juez los elimine de sus antecedentes si cumplen con los términos de su libertad condicional. Es probable que otros dos acaben entre rejas durante noventa días para evitar el cargo de delito mayor, y la suerte de uno de los acusados aún no se ha decidido.[115] (Los resultados finales se conocerán en diciembre de 2014.) Aunque las penas son menos duras de lo esperado, los acusados deberán soportar no obstante un agotador y caro calvario de tres años y, con los cargos de delito mayor pendiendo sobre sus cabezas, muchos pueden haber tenido (y probablemente continuarán teniendo) problemas para encontrar trabajo.

Todo este asunto está marcado asimismo por un doble discurso que ilustra la flagrante hipocresía de una sola corporación, PayPal, que persigue

a los manifestantes que participaron en la Operación Vengar a Assange. (MasterCard y Visa no quisieron procesar a los responsables.) En el tribunal, los abogados de PayPal calcularon que los daños ascendían a 5,5 millones de dólares.[116] Mientras tanto, en otros foros, funcionarios corporativos declaraban que «PayPal nunca quedó inactivo» o bien que el ataque solamente «ralentizó el sistema de la empresa, pero en una medida tan mínima que hubiera sido imperceptible para los clientes».[117] Éste es un ejemplo perfecto de cómo los actores corporativos no solo pueden continuar manifestando sus posturas sin problemas a través de multitud de canales, sino que también pueden participar en un doble discurso hipócrita y contradictorio mientras someten a los acusados a un proceso legal costoso y prolongado.

Finalmente, el debate sobre el DDoS quedó en gran medida obsoleto dentro de Anonymous. El éxito de la táctica pasó a identificarse con su capacidad para generar nuevos titulares. Esta dependencia de unos medios de comunicación obsesivamente cíclicos otorgaría una vida media muy corta a la visibilidad de acciones como Vengar a Assange. En Anonymous, que no eran ningunos tontos, lo vieron venir. Al dar por terminada la operación, el grupo anunció al mundo mediante un póster que «en el mejor de los casos les hemos dejado un ojo morado. El juego ha cambiado. Cuando el juego cambia, también lo hacen nuestras estrategias». A partir de diciembre de 2010, los ataques DDoS, con todos sus dilemas morales sin resolver, se convirtieron en un arma esgrimida solo ocasionalmente en un paquete de tácticas cada vez más diverso. Mientras tanto, en el pequeño país de Túnez, los acontecimientos comenzaron a avivarse y las acciones de un par de hackers, uno de ellos de AnonOps, pusieron en marcha unos hechos que, una vez más, lo cambiarían todo para el colectivo de colectivos: unos sucesos tan importantes como el nacimiento de la propia Chanology.

Capítulo 5

Anonymous en todas partes

A medida que 2010 daba paso al 2011 y la Operación Vengar a Assange se desvanecía lentamente, AnonOps comenzaba a promover otras operaciones. No se trataba de que AnonOps se estuviera escindiendo, sino más bien de que estaba floreciendo. Esta red de IRC se convirtió en la plataforma digital de moda entre los activistas de Anonymous de diferentes clases para organizar sus operaciones. Hacia finales de enero había operaciones y canales de IRC especializados en Italia, Irlanda, Venezuela, Brasil, Siria, Bahrein, Túnez, Egipto y Libia, junto con operaciones que no tenían una base fija, como la Operación Leakspin, una iniciativa para cribar los cables diplomáticos de WikiLeaks en busca de información de interés periodístico. Muchas de estas tentativas eran pequeñas pero, a pesar de todo, originaron nodos regionales dinámicos, siendo los más importantes los de Italia, Brasil y los Hispano-Anons. (En el momento de escribir este texto, Anonymous Italia ha filtrado documentos de la oficina del gobernador de la región de Lombardía, declarando que el político es “un gran corrupto cabrón” y acusándole, entre otras cosas, de permitir que delincuentes que distribuyen pornografía infantil laven su dinero a través de un banco de esa región italiana.[118]) Estas bolsas geográficas han prosperado y crecido hasta convertirse en comunidades fuertes. Aunque no muestran ningún síntoma de ralentizar su actividad, se han documentado muy pocos nodos regionales.[119]

La Operación Túnez pareció surgir de la nada. No fue hasta bastante más tarde que me informaron de las condiciones exactas que habían caracterizado su nacimiento; incluso años después, su fundador titubeó cuando le presioné para que me diese una explicación precisa: «Realmente

no sé por qué funcionó», insistió durante una entrevista. Dos geeks, Slim y Adnon (no es su seudónimo verdadero), que vivían en diferentes regiones del mundo y actuaban de forma independiente pero unidos en la creencia de que podían conseguir que el mundo fuese un lugar mejor, pusieron sus ojos en Túnez. Slim Amamou, un ciudadano tunecino que rondaba la treintena, esperaba que Anonymous participara dando publicidad a los problemas que agitaban a su país. Programador y bloguero, Amamou estaba fascinado con Anonymous y había dado charlas sobre el poder y la atracción de la política no identitaria. Amamou describía a Anonymous como el número cero: el número todopoderoso, el no-número. Era un ejemplo apropiado para un joven árabe, dado que fueron los matemáticos árabes quienes popularizaron el cero. Incorporando la idea de vacío e infinito, durante mucho tiempo, en Occidente el cero fue considerado como un concepto herético y solo introducido en las matemáticas y la filosofía durante el fermento intelectual y político de la Ilustración. Cero como el marcador supremo que rechaza una identidad concreta.

Mientras que Adnon, que vivía en la otra orilla del mar Mediterráneo, había *elegido* pertenecer a Anonymous, disfrutando de una vida privilegiada en una pintoresca e histórica ciudad europea sin temer la represión del gobierno, Amamou estaba arrinconado en una esquina del anonimato. Túnez se encontraba sometido a un régimen de fuerte censura: en 2010, este país de poco más de diez millones de habitantes ocupaba el puesto 164 de 178 en el Índice de Libertad de Prensa de la organización Reporteros Sin Fronteras (una clasificación anual que mide la libertad de prensa basándose en un cuestionario cumplimentado por organizaciones no gubernamentales, periodistas, juristas, académicos y trabajadores de los derechos humanos en numerosos países). Al igual que muchos tunecinos, Amamou utilizaba herramientas concebidas para evitar la censura para poder leer las noticias y hacer correr la voz. El uso de proxies y redes privadas virtuales (VPN) era un «conocimiento estándar entre la gente joven», me dijo. En Túnez, los geeks se veían impulsados a menudo por la necesidad y la voluntad de sobrevivir.

Muy pronto Anonymous llegaría a simbolizar la difícil situación general que vivían los tunecinos, manifestó Amamou en una entrevista, como un icono adoptado por igual por el joven hacker urbano y el habitante de las zonas rurales, debido al papel desempeñado por Anonymous en la

revuelta de su país. Muchos sabían que Anonymous había sido el grano de arena que engendró la perla de la atención de los medios de comunicación que habían estado ausentes en el inicio de su revolución. Era, sin lugar a dudas, una contribución modesta y segura, pero aún así una contribución crucial. El 8 de enero, una semana antes de la caída de Ben Alí, estudiantes tunecinos sentados en un patio rindieron tributo a Anonymous colocándose la máscara.

Amamou, quien ya desempeñaba un papel activo en la esfera de la política de Internet, no siempre actuaba de forma anónima. El 21 de mayo de 2010 fue detenido brevemente por secuaces del gobierno por su papel en la organización de una manifestación contra la censura en la red y que tendría lugar al día siguiente delante del Ministerio de Información. El 6 de enero fue arrestado nuevamente durante el momento álgido de las protestas. Me explicó: «Fui interrogado durante cinco días por la Seguridad del Estado... Es un lugar donde matan a la gente y creo —en realidad, estoy seguro, no es que lo crea— que me salvó Anonymous.» Los participantes de Anonymous, desde Tokio hasta Europa, se enteraron de su problema (la noticia circuló a través de los canales de Anonymous) provocando un aluvión de llamadas al gobierno de Túnez.

De modo que hacía tiempo que Anonymous ejercía su atracción sobre Amamou. Cuando su país se acercaba a una revolución total, Amamou quiso que el colectivo sin rostro se acercara más. De modo que "emplazó" a Anonymous a hacer acto de presencia. Pensó que si se iniciaba una operación, se obligaría a los medios de comunicación a dejar de ignorar a Túnez. Aunque reclamó la presencia de Anonymous, no era ningún ingenuo: «Anonymous no es tu ejército personal» es un lema que él conocía muy bien. «No puedes controlar a Anonymous», me dijo categóricamente, reprendiéndome después de que yo le preguntara qué cambiaría de Anonymous si pudiese. «Lo único que puedes hacer es tener la esperanza de que lleguen.» Afortunadamente, lo hicieron.

Y fue en parte gracias a Adnon, que tenía quince años cuando descubrió a Anonymous. Criado en Europa, pertenecía a una familia acomodada, aunque nunca lo dirías al salir con él. Fue una de las primeras personas de AnonOps que conocí "afk" ("lejos del teclado" en la jerga de IRC), un placer que desde entonces he disfrutado en múltiples ocasiones. De todo ese grupo, Adnon era el más modesto. Amable, tranquilo y

reflexivo, al principio me pareció un "tío normal", pero veinte minutos después de conocerle entendí por qué algunos de los hackers más veteranos se mostraban tan cariñosos y protectores con él.

En un caluroso día de verano, protegidos del inclemente sol debajo de las susurrantes hojas de un árbol, la conversación giró en gran medida en torno a preguntas y comentarios sobre Anonymous. Eso significó aproximadamente un 30 por ciento de cotilleo, un 20 por ciento de conspiración y el 50 por ciento restante de pedagogía sobre las tripas de Anonymous. La transición del chat virtual a la conversación cara a cara fue muy fluida. El mero hecho de encontrar a alguien de carne y hueso perteneciente a este ámbito representó un gran alivio.

Él se quejó de su aburrido y servil trabajo diario (aunque rico, no era un malcriado) y se animó al contarme algunas de sus muchas aventuras al aire libre montando en bicicleta o practicando piragüismo. A menudo muerto de aburrimiento en la escuela y habiendo pasado bastante tiempo online, se unió a AnonOps en otoño de 2010, durante la primera fase de la Operación Venganza. Me explicó: «Me decidí a participar porque había leído un artículo en alguna parte y pensé, '¡oh, tío, esos hackers son geniales!' Luego me di cuenta de que eran mucho más que eso.» Aunque distaba mucho de ser un hacker talentoso, era técnicamente competente, y se podría decir incluso que era un prototipo de geek.

Mientras navegaba en el barco de Anonymous, Adnon acumuló nuevas habilidades: protocolos de seguridad y bases de datos y gestión de servidores de red. Pero «las cosas más importantes que aprendí —dijo— no eran técnicas. El trabajo en equipo y la organización son impresionantes.» Era uno —de los cuatro que llegué a conocer— de esos organizadores e intermediarios fundamentales para que el reloj de Anonymous siguiera funcionando, un artilugio que se parecía más a los relojes blandos de Dalí que a un dispositivo suizo.

Durante buena parte del otoño de 2010, Adnon fue un ávido espectador de IRC, con intervenciones solo ocasionales en cuestiones organizativas. Pero chateaba, especialmente con otros operadores de canales como joepie91. Finalmente, a finales de diciembre, Adnon creó una propuesta con la ayuda de aquellos con quienes había hablado durante tantas horas. Esa propuesta cambió para siempre el curso de AnonOps.

Su sugerencia era simple: utilizar los recursos de Anonymous para

hacer pública la difícil situación que estaban viviendo los tunecinos que, en aquel momento, se rebelaban contra su presidente/dictador Ben Alí, quien ostentaba el poder desde 1987. En sus propias palabras: «Teníamos este canal #anonnews y estábamos tres de nosotros como moderadores... Uno de los tíos de allí, que creo que era tunecino, dijo algo así como 'Este chico se pegó fuego por lo que está pasando y hay algunas personas organizando pequeñas protestas. Sería genial hacer algo'.» Para entonces el gobierno tunecino ya había bloqueado los cables diplomáticos publicados por WikiLeaks, lo que creó un puente atractivo y urgente para un montón de geeks.[120]

Algunos asistentes a los canales insistieron al principio que era «demencial... ir contra un gobierno». Adnon lo dejó pasar. Una semana más tarde, en vísperas de Año Nuevo, Adnon estaba de vacaciones con su familia. Con la ventisca rugiendo en el exterior se escabulló para conectarse desde su habitación del hotel. Rechazó los argumentos de los opositores, impulsado por un sentido de la rectitud —y también por una dosis de información errónea y malentendida: «Yo, ignorante de la dimensión real de los anons 'moralfags', supuse que había miles de miembros activos y me dije, ¿por qué no?» Es verdad que había miles de ellos durante la Operación Vengar a Assange, pero el número real ascendía solo a unos centenares, y los que trabajaban específicamente en cuestiones técnicas y de propaganda eran incluso menos y seguían menguando. Pero él siguió presionando y, finalmente, consiguió convencer a una cantidad suficiente de Anons:

<Adnon>: Simplemente esparcimos la mierda fuera del enlace al canal #optunisia en todas partes
<Adnon>: la gente estaba aburrida
<Adnon>: fue una idea loca

Muchos asistentes seguían mostrándose escépticos. Tal como informó Quinn Norton para *Wired*, muchos «no creían que la operación o la revolución tuviesen ninguna posibilidad».[121] Pero resultó ser una de las operaciones más estelares del grupo, iniciando la transformación de Anonymous en Anonymous *Everywhere*. El grupo ya no estaba vinculado a cuestiones relacionadas con Internet como la censura y el intercambio de archivos.

Un par de días después de que Adnon resucitara la propuesta, recibió un mensaje privado (PM) en IRC de alguien en #internetfeds que ofrecía sus numerosos servicios: *defacement* ("desfiguración") de web, DDoSeo, hackeos. Tal vez esto fuese más fácil de lo que había pensado. El 2 de enero de 2011, en el amanecer de un nuevo año —siempre una señal de esperanza— Anonymous publicó la siguiente nota de prensa inaugurando #OpTunisia, traducida finalmente al francés, al árabe, al español y al italiano:

> Ha llegado la hora de la verdad. La hora de que la gente se exprese libremente y sea escuchada desde todos los rincones del mundo. El gobierno tunecino quiere controlar el presente con falsedades e información errónea para imponer el futuro ocultando la verdad a sus ciudadanos. No permaneceremos en silencio mientras esto sucede. Anonymous ha escuchado el reclamo de libertad del pueblo tunecino. Anonymous desea ayudar al pueblo tunecino en su lucha contra la opresión. Se hará. Se hará.
>
> Esta es una advertencia al gobierno tunecino: no se tolerarán los ataques a la libertad de expresión e información de sus ciudadanos. Cualquier organización implicada en la censura será nuestro objetivo y no será liberada hasta que el gobierno tunecino haya escuchado el reclamo de libertad de su pueblo. Está en manos del gobierno tunecino acabar con esta situación. Liberad la red y los ataques cesarán; mantened esa actitud y ésto será solo el principio.

El tigre consume cuatro pollos al día

Pero volvamos al inicio de la propia revolución. Mohamed Bouazizi, Nawaat, WikiLeaks y Chelsea Manning merecen nuestro agradecimiento por su gestación. En 2010, bajo el régimen de Ben Alí desde 1989, decenas de miles de tunecinos estaban oprimidos, viviendo en condiciones deplorables y aterrorizados mientras los abusos de los derechos humanos —tortura, censura y detenciones— se intensificaban en el país. Túnez no había visto protestas a gran escala desde hacía décadas, y sus numerosos

aliados occidentales, incluido Estados Unidos, destacaban al país como un modelo de estabilidad política y económica en una región árabe conocida por los conflictos y la incertidumbre reinantes.

De modo que cuando estalló la revolución —y cuando los principales medios de comunicación *finalmente* informaron sobre ella con seriedad— supuso una conmoción (al menos para los occidentales). Las manifestaciones provocaron una de las caídas de un régimen dictatorial más rápidas de la época reciente y se extendieron como una reacción en cadena a través de la región hasta convertirse en lo que hoy se conoce como Primavera árabe. Al igual que sucedió con tantos momentos revolucionarios, el análisis retrospectivo revela que había habido, a la vista de todos, la suficiente desesperación para encender una hoguera de desafío que ardiese durante semanas. Lo único que faltaba era una cerilla: en Túnez se presentaron dos.

Primero, el 28 de noviembre, cuando WikiLeaks hizo pública su primera tanda de 220 cables diplomáticos, tomaron la inteligente decisión de asociarse con activistas locales y medios de comunicación repartidos por todo el mundo. Uno de ellos estaba en Túnez: Nawaat. WikiLeaks les proporcionó cables específicos de Túnez. Tres miembros de Nawaat tradujeron los cables al francés y los publicaron bajo la banderola de TuniLeaks para que coincidiese con la importante revelación pública de documentos realizada por WikiLeaks. Nawaat trabajó también con geeks y hackers extranjeros para asegurarse de que su sitio web que contenía los cables permaneciera en la red, ante los decididos intentos del gobierno para censurarlos.

Los cables confirmaron lo que ya era de dominio público pero que, hasta entonces, no había sido documentado como un hecho probado: Ben Alí era corrupto hasta la médula, su régimen estaba también inmerso en la corrupción y su familia vivía en la opulencia mientras el resto del país luchaba para hacer frente a sus necesidades diarias. «La prueba ampliamente disponible de la corrupción y la hipocresía del gobierno, basada en un flujo incontenible de filtraciones, fue fundamental para agitar las llamas de la ira y la revuelta de los habitantes de toda la región», escribió Ibrahim Saleh, un experto en política tunecina.[122]

Muchos tunecinos leyeron estos cables, tomando debida nota del número exacto de pollos necesario para alimentar a una mascota tigre y de

las tres clases de zumos que se servían durante la cena, uno de los cuales era de kiwi, un fruto muy difícil de encontrar en el país:

> 12. (S) La cena estuvo compuesta de tal vez una docena de platos, incluidos pescado, filete, pavo, pulpo, cuscús de pescado y mucho más. La cantidad bastaba para satisfacer a un gran número de invitados. Antes de la cena se sirvió una amplia variedad de platitos junto con tres zumos diferentes (incluido zumo de kiwi, una fruta que normalmente no se consigue aquí). Después de la cena, se sirvieron helado y yogures helados que habían traído en avión desde Saint Tropez, junto con arándanos y frambuesas y frutas frescas y pastel de chocolate.
>
> 13. (S) El Materi [el yerno de Ben Alí] tiene un tigre de gran tamaño (*Pasha*) en su recinto, alojado en una jaula. Lo compró cuando el felino tenía unas pocas semanas. El tigre consume cuatro pollos al día. (Comentario: la situación recordaba a la de la jaula del león del embajador de Uday Hussein en Bagdad.) El Materi tenía personal en todas partes. Había al menos una docena de personas, incluido un mayordomo de Bangladesh y una niñera de Sudáfrica. (Nota: esto es extraordinariamente raro en Túnez y muy caro.)
>
> 19. (S) El dato más impactante de todos, sin embargo, era la opulencia en la que vivían El Materi y Nesrine. Su casa en Hammamet era impresionante, con el tigre sumándose a la impresión de "excesivo". Más extravagante aún es la casa que todavía está en fase de construcción en Sidi Bou Said. Esa residencia, a juzgar por su aspecto exterior, será semejante a un palacio. La construcción domina el paisaje urbano de Sidi Bou Said desde algunos puntos panorámicos y ha sido motivo de muchos comentarios críticos privados. La opulencia en la que viven El Materi y Nesrine y su comportamiento explican claramente por qué ellos y otros miembros de la familia de Ben Alí son detestados e incluso odiados por algunos tunecinos. Los excesos de la familia Ben Alí van en aumento.[123]

Segundo, el 17 de diciembre de 2010, tres meses después de que

Nawaat.org publicase los cables traducidos, un acto de desesperación ajeno a estos hechos desgarró el alma de la nación. Bouazizi —un joven vendedor ambulante de verduras— fue abordado por la policía, que le incautó su puesto ambulante por carecer de licencia y se negó a devolvérselo incluso después de que Bouazizi se ofreciera a pagar la multa. Su primer intento de recuperar su carrito fracasó. Unos funcionarios del gobierno de bajo rango se negaron incluso a hablar con él. Sintiéndose doblemente insultado y con una familia de ocho miembros a la que alimentar, Bouazizi se prendió fuego. Impotente y sin voz en ese momento, se convirtió un segundo después en alguien imposible de ignorar: pero al terrible precio de su vida.

Las protestas comenzaron en Sidi Bouzid, la ciudad donde residía Bouazizi, y se extendieron rápidamente en todas direcciones. La gente moría a manos de la policía y este hecho provocaba que más personas se unieran a las protestas. Takriz, un grupo experto en Internet contratado como una lista de mailing en 1999, se encargó de conectar a Internet a la juventud sublevada en las calles.[124] Aunque Takriz no tenía una relación directa con Anonymous, eran almas gemelas. Takriz, una red compuesta por unos pocos miles de personas, se niega habitualmente a cooperar con periodistas, esgrime la obscenidad como una táctica de choque y adopta orgullosamente el anonimato. En su cuenta de Twitter actual se puede leer: «Grupo de estudio/lucha cibernético tunecino & red de resistencia callejera desde 1998. ¡Libre, Verdadero & Anónimo —Takrizo Ergo Sum— Hacemos revoluciones!»[125]

Bouazizi murió a causa de las quemaduras el 4 de enero de 2011 y se calcula que al día siguiente asistieron a su funeral alrededor de cinco mil personas, muchas de ellas cantando, «Adiós, Mohamed, te vengaremos. Hoy lloramos por ti, haremos que lloren aquellos que causaron tu muerte».[126] Al día siguiente, el 75 por ciento de los abogados de la nación se declaró en huelga exigiendo el fin de la represión.[127] Tunecinos de todos los ámbitos de la sociedad —maestros, sindicalistas, estudiantes— se unieron a la lucha. Las protestan continuaron extendiéndose y la violencia policial se incrementó. Hacia el 13 de enero, docenas de periodistas, blogueros y activistas habían sido arrestados, y más de sesenta manifestantes habían sido asesinados. Hacia mediados de mes, Ben Alí decretó el estado de emergencia, pero la furia ya era imposible de contener. Sin embargo, al leer los principales medios de comunicación occidentales

de aquella época, uno apenas si se habría enterado de lo que sucedía en ese país.

«Después de todo, no tienen que llevar máscara para hacerlo»

La opinión pública norteamericana y europea tuvo las primeras noticias de las protestas tunecinas gracias a la publicación de una breve nota de Associated Press sobre los disturbios. El informe carecía comprensiblemente de detalles, ya que la revuelta acababa de estallar. Con el paso de los días, a pesar de que las protestas se intensificaban, la información en los principales medios de comunicación occidentales, con unas pocas y menores excepciones, seguía siendo tibia. El 9 de enero de 2011 (con Anonymous ya participando en Túnez y actuando en calidad de palomas mensajeras digitales para sacar la palabra y los vídeos fuera de las trincheras y ofrecerlos al público en general), la agencia AP publicó otra noticia, recogida por periódicos como *The New York Times* y *The Globe and The Mail*, que repetían como loros la postura de Ben Alí. «La gente que participa en estos disturbios afirma que están furiosos por la falta de empleo e inversiones, pero los funcionarios dicen que los disturbios son obra de una minoría de extremistas que intentan perjudicar a este país norteafricano.»[128] Ben Alí huyó del país menos de una semana más tarde, el 15 de enero de 2011.

Como parte de su campaña, Anonymous escribió la siguiente carta a los periodistas:

> Hemos observado que los persistentes disturbios en Túnez han pasado desapercibidos en general para las fiables redes de noticias occidentales. Es responsabilidad de la prensa libre y abierta informar de aquello que no puede hacer la prensa sometida a censura. Las manifestaciones públicas, así como las acciones emprendidas por Anonymous en solidaridad con los ciudadanos de Túnez, exigen la cobertura de los principales medios de comunicación.
>
> El gobierno tunecino, encabezado por el presidente Ben Alí, ha demostrado un nivel de censura escandaloso, no solo a través del

bloqueo de sitios web de los blogueros disidentes, sino también de sitios como Flickr y cualesquiera sitios web o fuentes de noticias que mencionaran a WikiLeaks. En una muestra de absoluto desprecio por el derecho garantizado a la libre expresión, durante las pasadas 24 horas funcionarios del gobierno tunecino han hackeado cuentas de correo electrónico y Facebook de cualquiera que haya llevado a cabo acciones catalogadas como “activismo” (que puede ser algo tan “peligroso” como organizar una protesta, o tan inocente como hacer comentarios en un foro de debates para un grupo relacionado con WikiLeaks). Cuentas completas de Facebook han sido requisadas por el gobierno tunecino, que ha llegado al extremo de cambiar las fotos de los perfiles por un barco pirata para burlarse de aquellos que defienden la libertad de expresión.

Anonymous, a su vez, ha lanzado ataques DDoS contra los sitios web del primer ministro tunecino y su gobierno corrupto, la bolsa de valores y el principal servidor de DNS de Túnez, logrando de este modo dejar inactivos muchos de los sitios web acabados en .tn. Además, hemos tomado medidas para asegurar que los tunecinos puedan conectarse anónimamente a Internet y acceder a la información que su gobierno no quiere que vean.

Ha habido una ausencia prácticamente total de cobertura destacada en los medios de comunicación. Preguntamos, ¿por qué una fuente de noticias como Al Jazeera es una de las pocas que cubre estas estremecedoras revueltas, mientras las demás permanecen en silencio? El mundo tiene la impresión de que a menos que los intereses económicos occidentales se vean comprometidos, a nuestros medios de comunicación nos les preocupa informar sobre ello.

¿Tal vez no lo sabían? Ahora que lo saben, pueden ayudarnos a difundir la noticia. Después de todo, no hace falta llevar máscara para hacerlo.

Atentamente,

Anonymous[129]

«TÍOS, CREEDME, LA CLAVE ESTÁ EN NO TENER EGO»

Pero Anonymous estaba haciendo algo más que fastidiar a los medios de comunicación dominantes para que hicieran su trabajo. El 2 de enero de 2011, un equipo técnico en #internetfeds renunció a sus vacaciones para trabajar sin parar. De hecho, Adnon me dijo que durante dos semanas apenas había dormido. Durante una entrevista explicó que la operación asumió un enfoque diferente de la Operación Venganza y la Operación Vengar a Assange:

<Adnon>: Con Túnez teníamos un plan
<Adnon>: Pensamos cuidadosamente qué hacer y cuándo en un pequeño grupo
<Adnon>: presentamos una lista de opciones en una votación
<Adnon>: luego llevamos el resultado de la votación
<Adnon>: No fue una decisión tomada por un grupo tan grande como en otras ops

OpTúnez supuso un cambio radical tanto en el ámbito interno como en el externo. Durante todo el otoño, múltiples grupos y canales secretos habían poblado Anonymous. Incluso Chanology tuvo que contar con *marblecake*, un grupo propio. Si bien aquellos que participaban en canales secretos ejercían un poder técnico y en muchos aspectos tenían el control, dependían no obstante de los que estaban en el canal público para conseguir sus objetivos. Las masas airadas del cuerpo político de IRC mantenían controlados a los grupos secretos, un mensaje que quedó claro cuando, a comienzos del otoño, las masas se levantaron en un linchamiento colectivo ante los intentos de #command de suspender los ataques DDoS en respuesta al Partido Pirata.

La gestión de OpTúnez fue diferente: desde el principio, un puñado de equipos más pequeños compuestos de hackers, creadores de propaganda y organizadores se hizo cargo de la operación y nunca la abandonó. No se trataba de que este modelo basado en equipos desplazara a otras modalidades de organización colectiva. Había otras operaciones simultáneas, algunas de las cuales estaban originadas en los canales

públicos sin participación de las camarillas. Y existía también un canal de IRC público vinculado a OpTÚnez que desempeñó un valioso papel.

El 2 de enero de 2011, un hacker llamado "rubik" (no es su seudónimo verdadero), que había estado trabajando en dos canales privados, apareció para anunciar que un sitio web tunecino había sido desfigurado (se han cambiado todos los seudónimos):

<rubik>: http://www.pm.gov.tn/pm/index.php—desfigurado
<OT>: ¡así se hace anons!!!!!
<OT>: ¡así jodidamente se hace!
<rubik>: ¡Un puto sobresaliente! Buen trabajo
<OT>: Habrá más, perras: P
<rubik>: http://www.marchespublics.gov.tn/ también.
<K-rad>: http://www.pm.gov.tn y http://www.marchespublics. gov.tn/ DES-JODIDAMENTE-FIGURADO!
<lafdie>: por cierto gracias a los lolcats: http://www.pm.gov.tn/pm/ index.php
<vvom>: http://www.pm.gov.tn/pm/index.php TOMA YA CABRONES

Un grupo de hackers había estado trabajando duro, cooperando como un equipo, durante algún tiempo. Sin embargo, la mayoría de los periodistas no pudo resistir la tentación de señalar la existencia de un "cerebro" o "líder," el arquitecto que evidentemente movía los hilos detrás de todos los demás. Irónicamente, una búsqueda en Internet de «líder de Anonymous» producirá al menos cuatro nombres diferentes. Finalmente, la mayoría de los periodistas identificó a Sabu y Topiary como líderes del colectivo, muy probablemente porque combinaron erróneamente su sólida presencia en las comunicaciones con el control organizativo (o dictatorial).130

Aunque muchos artículos señalaban a un "cabecilla" o "cerebro", la naturaleza exacta de lo que esto significa permanece en gran medida en el terreno de la especulación. Se deja al lector abandonado a su imaginación, vislumbrando tal vez a un malvado elitista sentado en un sillón de respaldo alto en algún palacio de hielo, que acaricia a un gato sobre su regazo mientras el eco de una risa profunda reverbera lentamente por las estancias. Adrian Chen dedujo, basándose en registros de IRC filtrados, que «Sabu desempeña el papel de líder, aplicando una disciplina unitaria mientras el resto de los miembros le apoyan».131 Y, sin embargo, el propio Chen contradice a continuación esta hipótesis dirigiendo la atención hacia un

hackeo conexo llevado a cabo por otro grupo de Anons sin la aportación de Sabu. Analizar un único registro buscando pruebas de la existencia de un líder es una acción tan eficaz como extrapolar todo el argumento de una película a partir de un único fotograma. No obstante, Charles Arthur del *The Guardian* cometió el mismo error y escribió, «durante algún tiempo después de los arrestos producidos en el Reino Unido, el único miembro visiblemente activo de LulzSec sigue siendo su líder, conocido en la red como Sabu, quien negó serlo pero simultáneamente emplea frases como 'mi equipo'».[132] Pero un contexto más amplio revela que Sabu se refería simplemente al canal #pure-elite que él mismo había creado hacía mucho tiempo y al que otros miembros de LulzSec describen como un canal «donde los amigos de LulzSec» podían pasar el rato.

Por lo visto, las iniciativas de los hackers, especialmente en el caso de Anonymous, tienden a ser dinámicas y fluidas, con múltiples individuos o incuso grupos trabajando de forma concertada. Lo que es verdad para una operación puede no serlo para la siguiente. En ocasiones, un hacker particularmente obsesivo genera, durante algún tiempo, un flujo de trabajo colectivo organizado. En otras ocasiones, caos y mala comunicación. De hecho, cuando entrevisté a Jeremy Hammond en prisión mucho tiempo después, se lamentó, «me gustaría que fuésemos más como RedHack, más disciplinados». RedHack, un grupo hacktivista con sede en Turquía, tiene una jerarquía clara, un líder y un portavoz, productos todos ellos de dieciséis años de organización y de una devoción compartida por las tácticas marxista-leninistas.

Tal vez Anonymous podría haber conseguido más si hubiese contado con un líder o con una jerarquía estática. Los hackers tienen tendencia a sufrir lo que me gusta llamar Trastorno por Distracción Geek, (TDG). Sin vigilancia, un hacker podría acabar fácilmente tirado en medio de un campo, rodeado de yaks, con una navaja de afeitar en la mano y preguntándose cómo diablos llegó allí (si entiendes esta referencia, ¡estás en peligro!). Pero es igualmente probable que Anonymous haya llegado tan lejos precisamente *porque* no tenía ningún jefe alrededor que le señalara un destino fijo. Cualquiera que sea el caso, el trabajo se desplegaba de forma orgánica: según quién estuviera en el canal, dependiendo de qué podía aportar cada participante y de la voluntad, en un determinado momento, de aprender algo nuevo —el elemento fundamental de la mayor parte de los

hackeos que acababan en éxito.

OpTúnez ilustra perfectamente todo este panorama. Imagina que estás en el IRC, como un Anon asistiendo al inicio de la operación. Es el 2 de enero de 2011 y estás trabajando directamente con activistas y hackers tunecinos que te proporcionan información veraz sobre una revuelta histórica. Estás en tu casa, sentado, prácticamente inmóvil excepto por los dedos que vuelan sobre el teclado; pero la información que recibes permite dar respuestas que pueden marcar una diferencia directa en el evento en cuestión, apenas a un paso de distancia de la gente que está sobre el terreno y lanza cócteles molotov. Tus contribuciones no serán necesariamente significativas en este proceso, pero no pueden ser ignoradas. Son personalmente útiles, un mecanismo de solidaridad y, en algunos casos, tal vez incluso una verdadera ayuda que protege de sufrir daños a los que están sobre el terreno. Todo esto depende de formas de cooperación cambiantes y confusas y prepara el escenario para que surjan organizaciones en torno a una idea particularmente buena, y se desmoronen incluso al más leve indicio de desacuerdo y de alternativas.

En ese momento había dos canales de IRC diferentes y privados que estaban activos simultáneamente, #opdeface y #internetfeds. En este último se llevaba a cabo el trabajo técnico pesado, mientras que en el primero se congregaban los organizadores. Un *gopher* (servicio de Internet que consiste en el acceso a la información a través de menús) llevaba las noticias del uno al otro. Algunos hackers estaban informados, mientras que otros iban llegando continuamente (se han cambiado todos los seudónimos):

> <rubik>: K-rad, ¿Algo bueno con PostgreSQL? [PostgresSQL es una base de datos]
> <rubik>: http://www.pm.gov.tn/pm/banniere/redirectb.php?id=54& idb=3’2&
> <K-rad>: rubik, nunca me he conectado con PostgreSQL, es incluso la primera vez que lo veo en una casilla para ser sincero
> <gibnut>: ¿por qué estamos golpeando a Túnez?
> <K-rad>: Porque acaban de aprobar una ley que dice que los medios de comunicación no pueden publicar lo que quieren
> <K-rad>: y les han prohibido mencionar a wikileaks
> <gibnut>: K-rad, ¡gracias!
> <gibnut>: es hora de ir a por Túnez entonces ;)

En otros canales, los usuarios sugerían llevar a cabo campañas de DDoS,

pero tanto en Anonymous como fuera, había quienes se enorgullecían de ser “verdaderos” hackers y rechazaban el DDoS como una herramienta mediocre (o incluso prejudicial para los auténticos hackeos, como veremos en un momento). Los verdaderos hackers encuentran las vulnerabilidades. La gente que simplemente ejecuta la LOIC está considerada por debajo del *hacker*, son meros *script kiddies*, o *skiddies* en su versión abreviada. Gibnut anuncia que tiene un “día-cero”, que es mucho más poderoso. Un exploit de día-cero, u *oh day* como la llama a veces la gente de forma jocosa, es una vulnerabilidad de seguridad previamente desconocida en una unidad de software. Se la llama día-cero porque es desconocida para el público —o los creadores de software que podrían repararla— por cero días y los que siguen. Un día cero es oro en polvo; cualquiera que conozca el día cero puede explorarlo una y otra vez hasta que sea reparado. Los días cero más codiciados proporcionan acceso a un ordenador o una red, razón por la que se venden con un elevado margen de beneficio en un floreciente mercado negro. Muchísimos gobiernos participan en este mercado éticamente problemático, incluido el gobierno de Estados Unidos, que, según el periodista especializado en tecnología Joseph Menn, «se ha convertido en el principal comprador en un próspero mercado paralelo donde hackers y empresas de seguridad venden herramientas para piratear ordenadores».[133] El gobierno estadounidense compra principalmente días cero a empresas privadas que «gastan decenas de millones de dólares por año solo en exploits».[134] Baste con decir que la noticia de gibnuts fue recibida con gran entusiasmo:

<gibnut>: veamos, que se joda la loic, les haremos daño de otra manera
<p-ground>: oh sí por favor
<gibnut>: tengo un exploit de día 0 enrutado contra openwebmail y lo controlan los servidores NIC de Túnez
<gibnut>: https://risala.ati.tn/cgi-bin/openwebmail/openwebmail.pl
<gibnut>: si podemos entrar en ese servidor podemos enrutar los nombres de servidores tunecinos .tn tld y controlar todo su espacio de Internet
<p-ground>: oh mierda
<gibnut>: redireccionar todo a wikileaks ;)
<p-ground>: la mierda se hizo real gracias a gibnut

Con este día cero, gibnut está sugiriendo que pueden comprometer el

nombre de dominios de Internet en Túnez (el NIC) y controlar todo el espacio de nombres de dominio de alto nivel (TLD) tunecino. Un ejemplo de un TLD es .com o .org. Cada país posee su propio TLD; el de Túnez es ".tn". Si los Anons son capaces de comprometer este registrador tunecino, pueden redirigir a todos los que intentan navegar a un sitio web que acaba en .tn hacia cualquier servidor que les apetezca. Gibnut, apelando al lulz, sugiere WikiLeaks. Aunque este exploit particular no facilita el acceso (por razones desconocidas), sí consiguió propagar un ansioso optimismo por las líneas laterales:135

<gibnut>: déjadme ver si puedo entrar... brb [vuelvo enseguida]
<p-ground>: Armad las cabezas nucleares tíos.
<p-ground>: Internetfeds está entrando.
<K-rad>: gibnut, :D genial <3
<K-rad>: pero primero necesitamos encontrar un bug allí
<jaggy91>: épico
<p-ground>: por alguna razón las cosas en este canal siempre acaban siendo épicas
<jaggy91>: lol
<rubik>: ah creo que tendremos que usar alguna chuleta para inyectar postqresql o algo así
<gibnut>: rubik, o descargar havij para windows
<K-rad>: http://www.marchespublics.gov.tn ES ALTAMENTE INYECTABLE:3 [existe al menos una vulnerabilidad que permite que un atacante modifique la base de datos del sitio de maneras distintas a las previstas]
<K-rad>: estad atentos al lulz
<3 <rubik>: :o
<rubik>: parece el ministerio de justicia, creo, idk [no lo sé]
<K-rad>: no lo sé pero ¡UN MONTÓN de sitios son vuln [vulnerables]!

Como sucede con muchos hackers, si no saben algo, lo aprenden solos:

<K-rad>: ¿conocéis el virus de postgres?
<rubik>: sí
<K-rad>: leí algo sobre postgres y estudié algunas DB [base de datos] de modo que ahora sé cómo inyectarlo:D
<K-rad>: estad atentos para descargarlo

K-rad se ausentó durante un rato, evidentemente para trabajar duro, y luego regresó con algunos resultados. K-rad accedió a una base de datos con mil

seiscientas filas (y, por tanto, entradas) y trató de descifrar las contraseñas. Primero disculpándose —«lo siento, tío, me está llevando tiempo porque nunca he hecho postgres SQL (lenguaje de consulta estructurado) y estoy tratando de escribirlo en un script para hacerlo más rápido»— y luego, dándose cuenta de que el DDoS existente era lo que estaba provocando la ralentización de la descarga de contraseñas. Imploró:

> <K-rad>: Que alguien le diga a optúnez QUE NO DDOS 193.95.68.156 está jodiendo mi descarga

Mientras que éste era un esfuerzo en equipo, otros hackers intentaban tener acceso de manera simultánea a través de otras posibles vulnerabilidades de seguridad. Descubrieron que si lograban acceder al shell, que permite un acceso de bajo nivel al sistema, podrían conseguir potencialmente los correos electrónicos del primer ministro de Túnez y luego filtrarlos. Rubik logró hacerlo pero, lamentablemente, solo encontró correo basura, aunque ello no detuvo el proceso de “apropiación”. “Own”, “0wn” o “pwn” un servidor significa básicamente que has logrado acceder al máximo nivel de acceso privilegiado y, a partir de ahí, tienes vía libre para hacer lo que desees con él. Puedes leer cualquier archivo, escribir a cualquier archivo, cambiar los procesos en marcha, inyectar tus propios procesos/código malicioso o, si te lo propones, borrarlo todo. Eres un “root”, el administrador total de la máquina, aunque no estés en absoluto físicamente cerca de la propia máquina. Por supuesto, los Anons desfiguraron el sitio, pero primero intentaron conseguir algunos correos electrónicos:

> <rubik>: conseguí acceder al sitio pero allí no hay nada
> <K-rad>: brb [enseguida vuelvo] tíos voy a prepararme una taza de té :3
> <gibnut>:http://www.marchespublics.gov.tn/onmp/upload/upload_ fichier.php?Field=document&type=document
> <gibnut>: ;]
> <gibnut>: tendré que acceder ahora o más tarde
> <rubik>: putamadre
> <K-rad>: será mejor ahora mientras el vapor de anti-tuni.gov sigue avanzando
> <rubik>: podríamos subir un shell supongo
> [...]
> <rubik>: qué shells queréis tíos;]
> <rubik>: yo tengo como 40

<K-rad>: maximizaría el efecto y la moral
<K-rad>: si podemos enrutarlo, ¡necesitamos filtrar también los correos electrónicos!
<K-rad>: ¡no solo desconfigurarlo!
<K-rad>: :D
<K-rad>: a tope con la filtración de correos electrónicos: D:D
<rubik>: encontré el shell
<gibnut>: www.marchespublics.gov.tn/onmp/upload/documents
<K-rad>: que alguien haga una elegante página de desfiguración de revancha, por favor :3

Mientras el equipo se preparaba para desconfigurar la página, K-rad anunció excitado que había un antiguo kernel instalado. El kernel es el componente fundamental de un sistema operativo, el punto de contacto entre el hardware y el software. Un antiguo kernel significa habitualmente que hay algunos exploits conocidos, de modo que casi siempre es una buena señal para alguien que desea comprometer una máquina:

<rubik>: aquí hay una página a desfigurar
<rubik>: http://pickhost.eu/images/0004/1986/anonymousdeface Túnez.jpg
<rubik>: si les gusta
<rubik>: :p
<K-rad>:**OOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOOOOOOOOOOLD KERN** FTW [por la victoria]
<rubik>: ¿root?
<duckie>: No está mal rubik
<duckie>: ¿Alguna posibilidad de que pudieras centrar el texto en la parte inferior?
<rubik>: no lo sé yo no lo hice
<rubik>: estoy trabajando en tor [red de anonimato]
<rubik>: ojalá tuviera una vpn [red privada virtual]

Duckie acababa de conectarse para ayudar. Finalmente quedó fuera porque carecía de suficiente capacidad de hackeo de bajo nivel, pero era un organizador e intermediario habilidoso, de modo que, de momento, se le permitió permanecer en el canal. Tenía una extraña capacidad para nombrar las operaciones y un raro nivel de percepción de los cambios constantes que afectaban a AnonOps:

<duckie>: ¿Hay algo que pueda hacer para ayudar que no implique entrar en el servidor?

<duckie>: rubik, he estado entrando y saliendo, se suponía que este canal llevaba mucho tiempo muerto
<K-rad>: duckie haz una página de desfiguración! :D?

Mientras #internetfeds se lanzaba a la caza de los correos electrónicos privados del primer ministro tunecino, había otro canal, #opdeface, que también trabajaba duro. Incluso en el canal elitista que era #internetfeds, muchos ignoraban la existencia de #opdeface. Entretanto, la búsqueda de correos electrónicos resultó infructuosa. En #opdeface, rubik hizo un resumen técnico del exploit que habían encontrado en #internetfeds.

Algunos Anons tunecinos descubrieron que un exploit podría funcionar en otro objetivo:

<OT>: Repito: el objetivo principal es ati [Agencia tunecina de Internet]
<OT>: Responsable directa de la censura
<mo>: he encontrado un exploit XSS en el sitio de ati
<a>: OT, lol, pensé que habías dicho que era en opchannel [un canal público]
<OT>: lol
<OT>: todavía no estoy tan colocado [...]
<rubik>: encontramos administrador accediendo a contraseñas para entrar en publicmarches.gov.tn, que ahora está en la misma casilla que pm.gov.tn
<vj>: creo que miramos el ministerio de comunicación como objetivo DDoS
<vj>: si estaba inhabilitado, no recuerdo por qué
<a>: le estoy echando un vistazo

Rubik, pensando que quizás conseguirían encontrar algunos correos electrónicos jugosos, les pidió ayuda:

<rubik>: puede alguien preparar una declaración
<rubik>: para la descripción de torrent
<rubik>: cuando consigamos correos electrónicos en pm.gov.tn
<rubik>: es decir, un mensaje a pm.gov.tn sobre sus correos electrónicos filtrados
<rubik>: pero todavía no
<rubik>: preparar una página de desfiguración
<rubik>: a menos que prefieran http://pickhost.eu/images/0004/1986/anonymousdefacetunisia.jpg
<rubik>: y preparar una descripción de torrent o un manifiesto

Finalmente, #opdeface se pronunció:

<vj>: Saludos desde Anonymous.
<vj>: hemos estado observando vuestro trato a vuestro propio pueblo y estamos a la vez enormemente tristes y furiosos ante ese comportamiento. Habéis declarado unilateralmente la guerra a la libertad de expresión, a la democracia y hasta a vuestro propio pueblo. Vuestro pueblo se manifiesta en las calles exigiéndoos rendir de cuentas y sus propios derechos, que habéis considerado erróneamente que estaba en vuestras manos quitárselos.
<vj>: Utilizaremos este breve momento de atención que hemos conseguido para enviar un mensaje claro y rotundo que esperamos que nunca se olvide. Recordad, recordad, que cuanto más presionéis, más personas se rebelarán contra vuestro gobierno. Como un puñado de arena en la palma de vuestra mano, cuanto más presionéis a vuestro pueblo, más se escapará de vuestra mano. Cuanto más censuréis a vuestro
<vj>: propio pueblo, más sabrá acerca de vosotros y sobre lo que estáis haciendo.
<vj>: Somos Anonymous.
<vj>: Somos el furioso avatar de la libre expresión.
<vj>: Somos el sistema inmunitario de la democracia.
<vj>: No perdonamos la censura.
<vj>: No olvidamos la libre expresión.
<vj>: Esperadnos–siempre.
<a>: buen material. Así lo haré/gente/ciudadanos/
<a>: suena más... profundo
<vj>: Utilizaremos este breve momento de atención que hemos obtenido para enviar un mensaje claro y rotundo que esperamos que nunca se olvide. Recordad, recordad, que cuanto más presionéis, más personas se rebelarán contra vuestro gobierno. Como un puñado de arena en la palma de vuestra mano, cuanto más presionéis a vuestro pueblo, más se escapará de vuestra mano. Cuanto más censureis a vuestro
<vj>: propio pueblo, más sabrá acerca de vosotros y sobre lo que estáis haciendo.
<vj>: Con ese espíritu revelamos a los ciudadanos de Túnez y al mundo un cache de documentos gubernamentales. Esperamos que arroje alguna luz sobre lo que el gobierno desea ocultar con tanta desesperación.

Rubik continuó actuando a modo de gopher entre ambos canales. Con el trabajo hecho hasta entonces, dio apoyo a uno de los miembros del equipo (que no era Sabu, por cierto). Otro Anon reprendió rápidamente esta alabanza individual por motivos éticos, y el propio K-rad restó importancia a este logro, un claro ejemplo de los discretos valores que incidían en Anonymous:

<rubik>: el crédito se lo lleva K-rad en este caso
<K-rad>: todo el mundo estaba en feds :D [feds se refiere al canal IRC #internetfeds]
<K-rad>: no olvidéis rm -rf su página admin login:D [rm -rf es el comando para borrar un directorio]
<K-rad>: ¡y rm -rf todo lo demás que podáis bajo esos permisos! :3
<Adnon>: Lo habéis conseguido tíos
<a>: no olvidéis a gibnut
<a>: y a todos los demás que trabajaron en segundo plano (=
<OT>: nada de nombres lol solo anonymus
<a>: sí, ofc [por jodido supuesto]
<a>: pero aquí... la gente que está aquí...
<nessy>: aunque actuamos en secreto
<a>: sigue estado bien. supongo (=
<OT>: tíos podéis creerme la clave de esto es tener 0 ego
<a>: solo estábamos dando reconocimiento
<a>: internamente :)
<OT>: lol
<alex>: eh
<alex>: ofc
<gibnut>: nada de nombres por favor. mi handle está caliente:)

Pues bien, aquí lo tenemos: hackers en plena faena. Es un trabajo en equipo prosaico, básico, pero también divertido y fantástico, al menos para los que intervienen en él. Solo he mencionado conversaciones pertenecientes a dos canales, pero el trabajo discurría a través de cuatro grupos diferentes, quizás incluso más, y es probable también que interviniera un panel de escritura colaborador donde se apuntaban los comunicados de prensa. Y debemos recordar que los canales públicos de OpTúnez, #propaganda y #command, estaban haciendo algo, cualquier cosa que fuese, al mismo tiempo. Muchos Anons se coordinaban también a través de mensajes privados.

En resumen, los tentáculos eran tan numerosos que la idea de un líder que lleva la voz cantante es ridícula: no una colmena (como a veces se denomina Anonymous a sí mismo), no una multitud sin estructura, y tampoco una jerarquía estructurada, sino alguna combinación de todas ellas.

«No te preocupes, yo también soy anonymous»

Como hemos visto claramente, las personas pueden destacar entre la masa gracias a sus aptitudes en cualquier situación particular. En OpTúnez, K-rad fue uno de estos destacados. Pero con el tiempo, las contribuciones individuales se fusionan entre ellas y el individuo queda sumergido. Sin embargo, teniendo en cuenta esta circunstancia, podemos apreciar el valor de observar a Anonymous desde la perspectiva opuesta: destacando a un participante, y su importante hackeo, con el propósito de corregir otro concepto erróneo persistente. Al mostrar el trabajo de tflow en OpTúnez, y analizándolo junto al de Adnon y Amamou, resultará evidente que el estereotipo del participante típico de Anonymus —blanco, de clase media, progresista y políticamente ingenuo —no se acerca en absoluto a la realidad.

Tflow (presentado más arriba con un seudónimo diferente) es un talentoso programador que se unió a Anonymous en otoño de 2010 y fundó #internetfeds como ala secreta de hackeo de AnonOps. Durante gran parte del otoño, tflow fue la llave maestra de #internetfeds, probando y vetando a hackers invitados sometiéndoles a tres preguntas de carácter técnico. Como uno de los contribuyentes técnicos más prolíficos de AnonOps, tflow tuvo la brillante idea de escribir un script antiphishing durante la OpTúnez. El phishing es, fundamentalmente, cualquier método que se emplea para conseguir detalles personales y privados —utilizando combinaciones de acceso y contraseñas o información obtenida de las tarjetas de crédito— y poder simular ser algo o alguien digno de confianza. Una técnica común consiste en enviar correos electrónicos falsos que parecen proceder del servicio de asistencia del proveedor de correos electrónicos de las víctimas, o de su banco, solicitando con urgencia que respondan con el nombre de usuario y la contraseña antes de que le cierren la cuenta. Una versión más sofisticada contiene un enlace que, cuando se activa, instala un keylogger (registrador de teclas) u otro tipo de software malicioso. La gente cae en la trampa de los ataques con phishing a un ritmo alarmante, lo que la convierte en una técnica particularmente lucrativa. Un estudio informático de esta técnica concluyó: «Los experimentos muestran una tasa de éxito superior al 70 por ciento en los ataques de phishing en las redes sociales.»[136] De modo que no debe sorprender que el régimen de Ben Alí utilizase un engaño de phishing, que incluía un script malicioso, para saquear los nombres de usuario y las contraseñas de las cuentas en las redes sociales de los

activistas tunecinos. La idea de tflow era conseguir un antídoto, un “script de phishing para derrocar al gobierno tunecino”.

El script de tflow es un excelente ejemplo de “hackeo ingenioso”, según una elegante definición de Jude Milhon, más conocida por su handle St. Jude, quien en una ocasión dijo: «Hackear es la elusión inteligente de los límites impuestos, ya sea por tu gobierno, por tu servidor de IP o por tu propia personalidad.»[137] El hackeo de tflow no era técnicamente sofisticado; escribió el código en menos de diez minutos y podría haberlo hecho en treinta segundos si hubiera estado más familiarizado con la tecnología subyacente. Era ingenioso simplemente porque identificaba una necesidad y *funcionaba*.

Antes incluso de que pudiera crear el breve programa, tenía que encontrar el script infractor. Para hacerlo debía encontrar a algún tunecino dispuesto a facilitarle el acceso informático remoto mediante la utilización de un programa informático llamado TeamViewer. A comienzos de enero se puso en contacto con un activista tunecino (con la excepción de tflow, se han cambiado todos los seudónimos):

<tflow>: anont
<anont>: tflow, sí
<tflow>: anont, ¿estás en Túnez?
<anont>: tflow, sí
<tflow>: ¿puedes pasarte a teamviewer para que podamos localizar la dirección de ip donde están funcionando los scripts de phishing para que podamos hackearlos? :]

Por supuesto, anontunisia hizo la pregunta obvia:

<anont>: tflow, ¿cómo sé que puedo confiar en ti?
<shaka>: tflow es muy fiable
<oggle>: tflow es un miembro de confianza
<Aa>: anont, creo que varias personas pueden avalar a tflow y yo seré una de ellas.

Puesto que, en realidad, la confianza es a menudo una cuestión de fe, tflow ofreció el consejo más sólido (y una persona recurrió a una “broma” estúpida y ofensiva):

<tflow>: anont, en tu pantalla puedes ver todo lo que estoy haciendo, si no te gusta

puedes salir
<shaka>: tflow es agradecido de la vieja escuela desde el principio
<k02>: confía en tflow ¡después de violarte siempre te da un caramelo!

anont respondió:

<anont>: A, tflow, shaka, OK. enviadme un mensaje privado

Ahora tflow pudo escribir el script. Simplemente, cambió las funciones en el script del gobierno de modo que no pudieran hacer nada. Un día más tarde, una vez que el script había sido escrito, cargado en línea y en proceso de ser descargado por miles de personas, tflow y anont se reunieron nuevamente en privado:

<tflow>: hey
<tflow>: ¿sigues aquí?
<anont>: sí
<tflow>: entra en teamviewer
<tflow>: quiero ver si el script funciona
[...]
<anont>: ¡buen trabajo! bien hecho
<anont>: :)
[...]
<anont>: hey
<anont>: tengo noticias
<tflow>: hey
<anont>: el periodista de aljazeera investigará el phishing con facebook, google & co
<tflow>: putamadre
<tflow>: también hay un artículo sobre ese tema aquí que lo explica bien http://www.thetechherald.com/article.php/201101/6651/Tunisian-government- harvesting-usernames-and-passwords
<anont>: sí
<anont>: lo envié anoche a varios medios de comunicación
<tflow>: bien
<anont>: yo también soy periodista :)
<tflow>: ¿enviaste también el script antiphishing?
<tflow>: ah
<anont>: sí
<anont>: no te preocupes
<anont>: yo también soy anonymous:D

Anont, periodista, sigue oculto en el anonimato, pero tuve la fortuna de conocer finalmente a tflow en Londres en julio de 2013, casi exactamente dos años después de su arresto por parte de la Policía Metropolitana Británica. Tflow se declaró culpable del cargo de utilización indebida de la informática, reconociendo haber conspirado para hackear a numerosas organizaciones británicas e internacionales, incluidos el Organismo de Lucha contra la Delincuencia Organizada Grave, la 20th Century Fox y News International. Puesto que en el momento de ser detenido era menor, consiguió librarse con una leve condena de servicio comunitario. La condena consistía, según me explicó en una entrevista, en «colocar etiquetas de precio a prendas que la gente donaba, ordenarlas en la tienda y rediseñar los escaparates».

Yo no había pasado mucho tiempo hablando con tflow, y nunca en privado precisamente. Su nombre era un elemento constante en mi pantalla y solíamos chatear, como parte de una conversación en grupo. Mientras participaba en una mezcla de conversaciones técnicas o filosóficas tflow era por lo general elocuente y afilado como un clavo. También podía ser arrogante, pero no era cruel, y a menudo se esforzaba por tener una percepción más amplia de las cosas. Tomemos, por ejemplo, la siguiente conversación de marzo de 2011 desarrollada en un canal de IRC para periodistas llamado “#reporter”. Un periodista acababa de iniciar sesión por primera vez y preguntó:

<reporter799>: ¿cómo funciona esto?
<reporter799>: soy muy nuevo en este asunto
<tflow>: es magia
<tflow>: brujería
<reporter799>: jaja
<reporter799>: bien, cuando dais una entrevista, ¿cómo funciona exactamente?
<Token>: Haz una pregunta y alguien la contestará
<reporter799>:¿solo eso, funciona así en general en este foro?
<tflow>: bueno, las leyes de la física producirán reacciones químicas en tu cerebro para decidir una pregunta, luego accionará los músculos de los brazos para que presiones las teclas que representarán tu pregunta. Luego, cuando presiones la tecla enter, se trasmitirá a través de los cables
<tflow>: sí.. sí solo tienes que hacer una pregunta aquí

<Token>: lol tflow
<reporter799>: ¿y solo mencionarla como “Miembro del Grupo de Anonymous”?
<tflow>: la mayoría de nosotros ha participado en operaciones de anonymus
<reporter799>: eso es alentador
[...]
<tflow>:¿para qué publicación/medio de noticias trabajas?
<reporter799>: soy free lance
<reporter799>: escribo para [X] y tengo mi propio blog
<reporter799>: te enviaré un enlace [lo envía]
<tflow>: de acuerdo
<reporter799>: Bien, ¿supongo que ahora puedo empezar a preguntar?
<tflow>: sin embargo no estoy seguro de cómo un blog de citas es relevante para este tema :P

Aunque estaba presente a menudo, resultaba difícil situarlo geográficamente. El inglés era obviamente su lengua materna, pero no daba demasiados detalles. Nunca se me pasó por la cabeza que, como en el caso de Adnon, pudiera ser un adolescente. Cuando le arrestaron el 19 de julio de 2011 y resultó ser un crío de 16 años, la conmoción se extendió a través de AnonOps. La gente estaba sorprendida porque sus colegas hackers le consideraban uno de los más listos del equipo; el trabajo en equipo no excluye la evaluación de capacidades y habilidades.

Puesto que en el momento de su arresto tflow era menor de edad, las autoridades no pudieron revelar su nombre, tan solo su edad. Me avergüenza admitir que cuando me enteré de que era británico y tenía 16 años, una imagen surgió súbitamente en mi mente. No era tan distinto de los «nihilistas, anarquistas, activistas, LulzSec, Anonymous, veinteañeros que llevan cinco o seis años sin hablar con nadie del sexo opuesto» descritos por Michael Haydn, el exdirector de la CIA y la NSA, en referencia a aquellos que luego apoyarían a Edward Snowden.[138] Lo que me vino a la mente fue la imagen de un niño desvalido y pálido cuyos progenitores ricos le habían enviado sin ninguna consideración a un internado desde su más tierna edad.

Resultó que, al cumplir los 18 años, tflow reveló ser Mustafa Al-Bassam y las fotografías confirmaron que no era blanco lechoso. Había llegado a Londres desde Irak con su familia cuando tenía seis años, huyendo del régimen de Saddam Hussein. Su padre es médico de familia, de modo que económicamente se inscriben en la clase media. Pero viven en

un vecindario pobre y saturado de inmigrantes en el sur de Londres y llevan un estilo de vida más propio de la clase trabajadora; sus padres, como muchas familias inmigrantes, ahorran en lugar de gastar. Cuando le insistí para que me hablara de su entorno, me explicó, con cierta incomodidad: «Vivimos en el uno por ciento inferior de las áreas del Reino Unido, económica y socialmente.»

Mi primer encuentro con él en Londres —a diferencia de mi primer encuentro con Adnon— fue tenso e incómodo, ya que no llevábamos cientos de horas de chateo previo para haber establecido cierta conexión. Esta desconexión se vio incrementada probablemente por el hecho de que él llevaba fuera de escena algún tiempo, ya que le habían prohibido utilizar Internet durante dos años. Por fortuna, los rayos de sol que se filtraban a través de la claraboya —el Reino Unido estaba disfrutando de un raro período soleado— contribuyó a suavizar el ambiente.

Continuamos nuestra conversación en línea. Un tema recurrente era la moralidad de la ley, algo que no debía sorprender teniendo en cuenta sus experiencias personales con el sistema de justicia. Un día hablamos sobre otro joven hacker, Aaron Swartz, atrapado por el sistema jurídico estadounidense (Swartz era uno de los cofundadores de reddit, uno de los sitios online más populares). Con tan solo 25 años, Swartz se enfrentaba a décadas de prisión —una pena de 35 años— y hasta un millón de dólares de multa por haber descargado documentos académicos de JSTOR, el archivo académico disponible para todos los miembros de la red del Instituto Tecnológico de Massachusetts (MIT).

Si Swartz hubiera sido declarado culpable, es poco probable que le hubiesen encarcelado durante tanto tiempo. Pero la cantidad de cargos contra él y la posibilidad de pasar tantos años entre rejas fueron utilizados por los fiscales para que negociara un acuerdo de culpabilidad y aceptara un cargo de delito mayor. El dato que resulta incluso más llamativo en este caso es que Swartz no “hackeó” en absoluto el sitio web de JSTOR; y JSTOR ni siquiera presentó cargos. Es verdad que el MIT tuvo que emplear algunos recursos en este asunto, pero no resultó gravemente perjudicado en absoluto. Sin embargo, el fiscal principal, Stephen Heymann, tuvo la osadía de comparar «al precursor de Internet con un violador y sugirió que había ‘revictimizado sistemáticamente’ al MIT al no aceptar un acuerdo de culpabilidad», según escribió Ryan Reily del *Huffington Post*.[139]

Quizás podría haber sido declarado culpable de haber invadido una propiedad privada; Swartz escondió un ordenador en un armario en el campus y lo conectó directamente al sistema del MIT. En algunas ocasiones, los administradores de la red del MIT le habían expulsado de la misma, sin duda en un intento de impedir que descargase más que un determinado número de artículos. Pero, incluso si algunas de sus acciones fueron ilegales o vulneraron algunas reglas, desde una perspectiva moral podríamos decir que la descarga de artículos académicos, muchos de ellos investigados y redactados gracias a los impuestos del contribuyente, no merecía en absoluto una condena a 35 años de prisión y un cargo de delito mayor, por no mencionar un costoso juicio sufragado también por los contribuyentes. Swartz, desesperado y acosado por la fiscalía, se quitó la vida el 6 de enero de 2013.

Un día, mientras chateaba con Al-Bassam sobre este caso, mencioné un artículo escrito por un profesor, Hal Abelson, que había presidido un comité que investigó el papel del MIT en este asunto. Abelson absolvió al MIT y describió a Swartz como «peligrosamente ingenuo con respecto a la realidad del ejercicio de su poder técnico, al extremo de que acabó por destruirse a sí mismo».[140] Horrorizada, respondí en un popular techblog: «Aquí la verdadera ingenuidad es la de Abelson. Su omisión en culpar a la injusta, agresiva y excesiva fiscalía federal, en vez de limitarse a tacharla de ‘vigorosa’, fue inaceptable porque utilizó un adjetivo que debería reservarse para un entrenamiento deportivo.»[141] Al-Bassam contestó: «’Peligrosamente ingenuo con respecto a la realidad del ejercicio de su poder, al extremo de que acabó por destruirse a sí mismo’ es una afirmación que debería aplicarse a la fiscalía, no a Aaron Swartz.»

Al-Bassam —tflow— había experimentado de primera mano la fuerza de la ley llamando a su puerta, y lo había hecho después de participar durante meses en acciones directas por causas en las que creía. No es sorprendente que las sensibilidades de la juventud sean la causa de tanta energía política creativa. Una energía de esa magnitud debe resultar más difícil de mantener cuando nuestro idealismo choca contra la horrenda realidad de los problemas que atormentan a nuestro mundo, coincidiendo con la carga cada vez mayor de responsabilidades cotidianas. Pero si el idealismo juvenil hace que alguien intente afrontar la enormidad de nuestros problemas, entonces necesitamos más “ingenuidad” juvenil, no

menos.

DESMONTANDO TÓPICOS

Adnon, tflow y Slim son tres activistas de Anonymous. Anonymous no es el club de los chicos estadounidenses blancos de clase media que todo el mundo se imagina. Las cifras resultan imposibles de precisar, pero los Anons que conocí y aquellos que han sido desenmascarados por las detenciones conforman un grupo multicolor (por cierto, multicolor es la vestimenta embaucadora, la prenda multicolor del bufón de la corte). Si, además de estos tres hombres, tenemos en cuenta el grupo de hackers con el que Al-Bassam trabajó en #internetfeds (y más tarde en LulzSec) conocidos ahora a causa de los arrestos, la heterogeneidad se vuelve más pronunciada. En sus filas había un puertorriqueño que vivía en un imponente complejo de viviendas públicas en Nueva York (también era traficante de drogas ocasional y padre adoptivo de sus primos); dos estudiantes irlandeses de química, uno cuyas ideas políticas estaban influidas por su padre, miembro del Ejército Republicano Irlandés (IRA) y que había pasado seis años en prisión; un escocés, que durante buena parte del tiempo que participó en Anonymous vivió en la remota isla de Yell; y un tío de 25 años, Kayla, que sirvió en el ejército británico en Irak y en la red se expresaba como una mujer.

Es probable que algo relacionado con el entorno de los seudónimos favoreciera este cosmopolitismo. Gracias al ocultamiento de marcadores de identidad personal, como etnia, clase y edad, se abren todo tipo de posibilidades. Los estudios confirman que tendemos a buscar a aquellos que nos resultan familiares (o similares a nosotros), y el compañerismo que propicia la identidad compartida no es algo de lo que burlarse ni descartar.[142] No obstante, también es importante crear y experimentar con espacios que silencian los marcadores de clase, edad y antecedentes para ayudar a formar conexiones que de otra manera no serían posibles. En cierto sentido, podría ser que la propia pertenencia autoadmitida a Anonymous se convierta en una identidad compartida suficiente para potenciar estas conexiones.

Si bien podemos mostrar sorprendentes ejemplos de diversidad dentro

de Anonymous, esto no significa decir que *no* carezca llamativamente de heterogeneidad. En especial cuando se trata del género: aunque Anonymous presumía de contar con participantes y organizadoras femeninas clave (como el caso de darr, presentada antes en este libro, y el de una combativa activista llamada Mercedes Haefer, cuyas acciones examinaremos pronto en profundidad), el único hacker "femanon" (miembro femenino de Anonymus) en LulzSec resultó ser un tío que se hacía pasar por mujer, Kayla.

Anonymous refleja las desigualdades estructurales que prevalecen en el mundo de la informática. Aunque la mayoría de los campos STEM (Ciencia, Tecnología, Ingeniería y Matemáticas) han reducido la brecha relativa al género, no es el caso de la informática. De hecho, el pico de igualdad en la matriculación universitaria se produjo hace más de veinte años, cuando el 37 por ciento de los títulos universitarios en informática otorgados en 1985 los obtuvieron mujeres. Actualmente el número ronda el 20 por ciento.[143] Y si bien las cifras son más difíciles de determinar para el ámbito del hackeo (considerando la naturaleza informal de muchas asociaciones), todos los indicadores apuntan a tasas de inclusión incluso inferiores.[144] En algunos sectores, como el software libre y de código abierto, muchos proyectos respondían a iniciativas destinadas a incrementar la diversidad.[145] Pero en el escenario de los sombreros negros, solo he conocido a una hacker y todos los demás que he conocido o de quien haya oído hablar son aquellos que han cambiado de género, algo que es —y quizás, para muchos, sorprendente— más común de lo que pueda imaginarse. (En cambio, es importante destacar que —por la razón que sea — las mujeres son más comunes en las comunidades dedicadas al troleo.) Aunque no existen estudios formales sobre género en el submundo de los hackers, la escasez de mujeres se debe probablemente al resultado combinado de fuerzas estructurales, riesgos legales inherentes a la actividad y la mentalidad de "club de tíos", insular y arrogante, dentro de la comunidad establecida.[146] En ocasiones, al escuchar el constante menosprecio de las contribuciones femeninas por parte de algunos Anons, me he encontrado preguntándome, «¿Se trata de sexismo o simplemente de troleo?», a sabiendas de que tal distinción rara vez es precisa.

Ser precisos en el tema de la diversidad y las dinámicas de género nos permite plantear preguntas más interesantes: ¿Por qué, por ejemplo, las

juergas de intercambio de géneros, los hackers homosexuales y los trols femeninos son categorías comunes y abiertamente aceptadas, pero en los círculos técnicos la participación femenina sigue siendo baja? Algunas identidades son aceptadas, mientras que otras siguen siendo vistas con escepticismo.

Desmontar estereotipos permite asimismo una mayor valoración de las motivaciones que muestran muchos de estos participantes. Podemos no estar de acuerdo con las tácticas —hackear, DDoSear, doxear— pero deberíamos diferenciar estas herramientas y su importancia a partir de la composición del propio Anonymous. Una y otra vez pude comprobar que los participantes actuaban con convicción política y es probable que algunos de ellos fuesen recién llegados a la arena política.

Esta realidad se pierde por completo si entendemos a Anonymous a través del fetiche bruto de los estereotipos. Muchos periodistas que me han entrevistado como “experta académica” preguntan, de un modo u otro, sobre «la clase de persona que ingresa en Anonymous». Aunque sea la respuesta que nadie quiere escuchar, a menudo contesto que no hay ninguna clase, excepto, nuevamente, que muchos tienden a ser geeks y hackers. Aquellos que se identifican como parte de Internet muestran una gran diversidad en cuanto a antecedentes, intereses y sensibilidad política. Pero detrás de la pregunta, quien la formula probablemente tiene un estereotipo en mente: joven estadounidense socialmente alienado, blanco, indignado, libertario. Y si asumimos que el hacker y geek predeterminado es generalmente varón, de clase media, libertario y blanco, entonces resulta mucho más sencillo tratar las intervenciones políticas de los hackers como juveniles y sospechosas, surgidas de una base de angustia adolescente, no del deseo de una acción política escrupulosa.

Capítulo 6

“Moralfaggotry” en todas partes

<Anonymous9>: En realidad hay algo que me deja un sabor agridulce
<Anonymous9>: Biella está aquí para hacer una investigación universitaria
<Anonymous9>: No puedo evitar tener la sensación de que tan pronto como haya escrito su tesis o cualquiera que sea su proyecto, no tendrá ningún otro motivo para seguir aquí :(
<Anonymous9>: Creo que no se da cuenta de cuánto ha contribuido a Anonymous
<Anonymous9>: Aun cuando no se vea necesariamente a sí misma como parte de esto

Este registro de chat de 2011 de un importante organizador y periodista de Anonymous me lo pasó alguien en 2013. Después de leerlo me sentí invadida por un cúmulo de emociones y recuerdos. Ese breve texto me recordó de qué manera el ciclo vital antropológico básico —el distanciamiento de la entrada inicial, seguido de la emoción de encontrar tu lugar y el doloroso final de la extracción— caracterizó mi investigación sobre Anonymous. La predicción de Anonymous9 era acertada. Una vez acabada la Operación Túnez me impliqué profundamente con Anonymous, y esta relación complicada se ha ido desvaneciendo con el correr del tiempo, especialmente cuando empecé a escribir este libro. Poco después de haber leído esta conversación filtrada aseguré a Anonymous9, uno de mis más íntimos confidentes de Anonymous, que seguiría siendo mi amigo aun cuando yo me dedicase a otros temas de investigación (pero solamente con la condición de que comprendiera que he dejado de ser una estudiante universitaria).

Las declaraciones de Anonymous9 me recordaron también que bastó el mes de enero de 2011 para dejar de ser una *outsider* confundida y

convertirme en una persona semi enterada. Esta transformación fue suscrita por las largas horas que dediqué a la investigación: cinco horas diarias en la red —como mínimo— todos los días de la semana. Sintonizaba simultáneamente entre siete y diez canales de IRC, observando y absorbiendo las idas y venidas de Anonymous. Por otra parte, pasaba aproximadamente diez horas por semana realizando entrevistas con los medios de comunicación sobre el tema de Anonymous. En dos años hablé con más de ciento cincuenta periodistas. Como resultado de todo esto, me corresponde ahora el dudoso honor de poder informar más y mejor sobre el IRC a los periodistas que cualquier otra persona en el mundo.

Con el paso del tiempo, el vértigo que me producía moverme a través de esa enorme cantidad de datos, día tras día, fue reemplazado por un sentimiento de pertenencia. Comencé a participar en los debates y pronto fui conocida, y más o menos aceptada, en varios canales y subcomunidades que surgían como las setas después de una lluvia abundante y generosa. Ya no estaba perdida en el bosque sino que me había convertido en parte del bosque. Como sucede con todos los bosques, el peligro acechaba en algunas zonas, pero al menos fui también cada vez más consciente de dónde se podían encontrar las partes más atractivas. Y descubrí que mi hogar se había convertido en el canal de IRC de AnonOps llamado #reporter.

La adaptación a mi nuevo hogar estuvo muy lejos de ser una transición fluida. Por muchas veces que me mentalizara para decir alguno, hablar sin reservas, presentarme tipo ahora, en este preciso instante… al final siempre acababa cediendo. Durante semanas me aterró abrir la boca, temiendo, simplemente, ser expulsada del canal y perder así una oportunidad increíble. Este grupo de Anons, a diferencia de los que formaban parte de Chanology, era duro y pendenciero. Había observado, completamente absorta, cómo a otros les expulsaban del canal por haber vulnerado algunos códigos éticos que para mí no estaban tan claros, y también –lo que resultaba incluso más agobiante– por ningún otro motivo que el lulz.

No fue hasta comienzos de enero de 2011 que hablé sin reservas por primera vez. Y no fue una acción del todo voluntaria. Al parecer, de manera absolutamente inesperada, repararon en mi presencia. Yo había estado observando desde una posición protegida, nadie me prestaba ni una pizca de atención, hasta que, de pronto, fue como si el ojo sin párpado de Sauron hubiese desviado la mirada hacia mi esquina de la habitación, derritiendo

las sombras que me ocultaban para bañarme en un intenso rayo de luz. En aquel momento me encontraba lejos del ordenador preparando algo de comida en la cocina. Cuando regresé encontré esto en la pantalla:

<Topiary>: ¿Puede alguien aquí confirmar a biella?
<q>: yo hablé hoy con ella pero...
<m42>: ¿la conoces q?
<q>: si ella me enviara un DM [mensaje directo] en twitter, podría.
<m42>: "biella está ausente: no estoy aquí en este momento" y no hay ninguna @ en ninguno de los 7 canales...
<q>: sí, si se trata de la biella de twitter, he hablado con ella antes
<Topiary>: Es posible que pronto necesitemos disponer de periodistas desde aquí.
<m42>: ella puede volver más tarde
has sido expulsada por q: (hola biella, ¿podrías enviarme un DM por twitter por favor? ¡Gracias!)

El corazón se me salía del pecho. Lancé un gemido. Es terrible que te expulsen de un canal. Eso significa que ya no puedes ver lo que está pasando y no sabes por qué te han despedido sumariamente y sin poder defenderte. Es una situación lamentable —tienes que preguntarte qué dicen sobre ti cuando no estás— y no estás segura de si permitirán que regreses. Podrías ser objeto de acciones "z-lined" o **"**q-lined," unas acciones que los operadores pueden llevar a cabo para excluir de manera permanente tu dirección de IP de toda la red de servidores, lo que significa desaparecer de todos los canales al instante. Afortunadamente, no era eso lo que tenían en mente. No me prohibieron que volviese a entrar en el canal. Diez minutos más tarde, devorada por la ansiedad, entré nuevamente en el sistema:

<biella>:hola q Topiary
<biella>:lo siento estaba cocinando
<biella>:esta soy yo
<biella>:http://steinhardt.nyu.edu/faculty_bios/view/Gabriella_Coleman
<biella>:he remitido a muchos periodistas a esta dirección
<biella>:estoy escribiendo/haciendo una presentación sobre Anonymous

Me respondieron inmediatamente:

<Topiary>: Hola biella, me disculpo por la patada.

<biella>: no, está todo bien
<biella>: me diste una advertencia razonable :-) y yo he sido demasiado, demasiado vaga
<biella>: más de lo que me gustaría
<Topiary>: habitualmente aquí somos muy estrictos y a veces un poco paranoicos con los usuarios no identificados.
[...]
<Topiary>: Me gustó lo que leí en tu enlace. ¿Qué aspectos de Anonymous tratarás en tu presentación?
<q>: biella, ¿puedes enviarme un DM en twitter?
<Topiary>: Desde luego espero leer tu trabajo.
<biella>: genial Topiary y empezaré con 1) si estoy equivocada/desactivada por favor contactadme. Estoy siempre abierta a los comentarios
<biella>: q, ¿cuál es tu cuenta de twitter?
<biella>: yo soy https://twitter.com/#!/BiellaColeman
[...]
<biella>: me alegro de que la tengas y no seré perezosa ni me conectaré aquí con frecuencia sin una buena razón
<biella>: bien ahora os dejaré a todos y volveré cuando tenga preguntas. En realidad tengo preguntas pero todo el mundo me está dando la lata para que vaya a cenar
<Topiary>: Pareces bastante práctica, me alegro de que estés informando sobre nosotros. Que disfrutes de la cena.
<Trivette>: estoy de acuerdo
<biella>: gracias Topiary, de acuerdo, hablamos más tarde
<q>: sí, solo puedo decir cosas buenas sobre biella. Solo quería estar seguro de que era la misma:)

¡Uf! Ahora que lo pienso, fue más como *¡UFFFFFFFFFFFFFFF!* Fue uno de esos momentos clásicos de éxito o fracaso. Si ellos hubiesen dicho que era inútil o sospechosa, habría significado mi final o, al menos, habría convertido la perspectiva de confianza y acceso en una gesta hercúlea. Los que participaban en #reporter tenían más autoridad que el Anon medio. Sus opiniones contaban.

Tal vez mi aceptación incruenta merece más explicaciones. Recuerdo que llevaba dos años investigando el Proyecto Chanology. Si bien la cultura política de AnonOps era diferente de la de los cruzados de la antiCienciología, existía una conexión cultural suficiente, de modo que cuando los participantes hurgaron en mi trabajo, la situación me resultó familiar. A partir de mis videoconferencias, sobre todo, no resultaba difícil

percibir el grado de simpatía que sentía por Anonymous, suficiente al menos como para determinar que yo disfrutaba del lulz.

Y no estaba sola. Había una confederación de aproximadamente media docena de *outsiders* a los que se les permitía el acceso extra a cambio de que hiceran de portavoces de Anonymous en los medios de comunicación. Un hacker convertido en periodista llamado Steve Ragan se encargaba de distribuir los artículos técnicos más detallados y matizados relacionados con Anonymous para el *Tech Herald*. Una periodista especializada en temas económicos para la revista *Forbes*, Parmy Olson, reprodujo series de noticias hasta convertirse finalmente en la periodista privada de LulzSec. Dos de sus miembros, Sabu y Topiary, le soltaban todo lo que sabían, reconociendo incluso —era casi increíble— que estaban infringiendo la ley. Los informes completos de Quinn Norton, que escribía para Wired.com, brillaron con luz propia durante el movimiento Occupy Wall Street, y Anonymous coincidía en el 99 por ciento. El cineasta Brian Knappenberger pasó más de un año entrevistando incansablemente a más de cuarenta Anons en el IRC, por vídeo chat y en persona, para un largometraje documental. (Brian y yo nos uniríamos finalmente en el empeño, que fracasó estrepitosamente, por conseguir filmar a Sabu.) Asher Wolf, una extraordinaria dama geek, habló con muchos Anons entre bastidores y consiguió, como nadie más fue capaz, capturar su *esprit de corps* en fragmentos de 140 caracteres o menos en Twitter. Amber Lyon, periodista que trabajaba para la CNN por aquel entonces, obtuvo una puntuación especial por haber llevado a cabo la mayor acción anti-Internet que haya podido realizar cualquiera de nosotros: atravesó a pie un remoto paso montañoso desde el estado de Washington hasta la Columbia Británica acompañando al hacker fugitivo Commander X (Christopher Doyon) cuando huía de Estados Unidos para evitar la prisión.

Los contactos de Anonymous con figuras conocidas e investigadores de los medios de comunicación son tan contradictorios y variados como el propio colectivo. La mayoría de los participantes trabajaba con los periodistas con todo el respeto y la transparencia que la naturaleza clandestina de Anonymous permitía. El objetivo principal, normalmente, era obtener publicidad para sus causas, por ejemplo expresar el descontento político en Túnez, pero también buscaban, siempre que era posible, gestionar cuidadosamente su propia imagen. En algunas ocasiones, el

objetivo también era trolear a un periodista determinado.

La gestión de la imagen o el troleo contaban con la ayuda de algunos publicistas propios proclives a elaborar contenidos destinados a ambos objetivos y que poblaron #reporter junto a periodistas y *outsiders* como yo misma. Dos de ellos en particular eran conocidos por hablar con los periodistas con mucho estilo: Topiary, que finalmente reveló ser Jake Davis, de 18 años y habitante de las remotas Islas Shetland escocesas (autodescrito en su perfil de Twitter como un «simple bromista convertido en pretencioso seto de jardín») y Barrett Brown, un tejano rubio de piel clara cuya habitación estaba llena de libros y que tenía un lince embalsamado que parecía ir a saltar de la pared en cualquier momento. Durante la OpTúnez, tflow había invitado a Topiary al santuario interno y demostró ser tan hábil tejiendo propaganda deliciosa alimentada por el lulz que se quedó como uno de sus miembros principales. Después de que Brown escribiera un breve artículo alabando a Anonymous, Gregg Housh (uno de los miembros originales de marblecake) le fichó para la causa.

Topiary y Barrett Brown eran asimismo embaucadores residentes de AnonOps, cada uno con una marca distintiva para las artimañas digitales. Inspirado por los dadaístas y los situacionistas, bromistas del arte de vanguardia del siglo XX, Topiary encontró su don en encadenar 140 caracteres de brillante sinsentido y absurda manipulación de los medios de comunicación. En el canal de los periodistas, Topiary presumía en voz alta de exploits y planes:

> <Topiary>: He hecho antes una entrevista hablada con estos tíos, son buenos, trabajan a través de Skype
> <Topiary>: Les dije que teníamos más de 9.000 miembros y les hice perder el juego, deberías hacerles un bel-air
> <Topiary>: O algo así
> <Topiary>: De todos modos, acabo de hablar con un monstruoso homogay llamado Andy que está redactando nuestras últimas gamberradas faxeadas

Topiary, que contaba con la admiración de muchos Anons, era un bromista enmascarado que había adoptado la seudonimia utilizada casi de forma unánime por sus colegas. Su nombre no se hizo público hasta después de su arresto. Por otra parte, no he incluido el apodo encubierto de Brown porque no tenía: era simplemente Barrett Brown —en ocasiones semidesnudo,

como podréis ver, pero siempre Barrett Brown. Asumió la función de portavoz de Anonymous en el invierno de 2011 y la conservó hasta mayo, cuando las oleadas de críticas le empujaron a apartarse. También cumplió el papel de bufón de la corte de AnonOps. Como cualquier embaucador que se precie, disfrutaba de baños de espuma realmente calientes mientras tomaba vino tinto (presumiblemente barato). Después de anunciar sus planes en Twitter —«Voy a buscar un poco de vino tinto. Cuando regrese dentro de 15 minutos tendremos un baño de espuma en directo»[147]—, los espectadores podían conectarse a Tinychat, un servicio de vídeo chat en directo, y verlo semisumergido en el agua mientras le lanzaban comentarios ofensivos y troleros; en este caso, "bromas de violador".

Al llegar con su nombre a la espalda, fue informalmente excluido por haber infringido una regla original de Anonymous (insinuada en el propio nombre): llamar la atención e intentar atraer la fama sobre el propio nombre es el máximo tabú. Brown intentó ocupar de manera iconoclasta un lugar a medio camino entre zona y estatus. Actuaba como *insider* pero nunca se ocultó. Su presencia fue tolerada durante tanto tiempo porque aportaba un trabajo considerable tanto a la red como a la causa superior. Periodista de profesión, Brown era experto en azotar a los poderosos con textos irónicos, mordazmente paródicos. En un número de la revista *Vanity Fair* donde se elogiaba al periodista de investigación Michael Hastings (hoy fallecido) –conocido por haber hecho un perfil poco favorecedor del general estadounidense Stanley McChrystal en la revista *Rolling Stone* y que provocó la caída del militar–, Brown sugirió burlonamente, «McChrystal habría hecho mejor en hablar con Thomas Friedman, que es tan graciosamente ingenuo que en 2001 declaró que Vladimir Putin era una fuerza del bien a quien todos los estadounidenses deberían estar '*rootin'*'–"aclamando"–, un término que escogió porque rima con Putin.»[148] Brown tenía un conocimiento excelente de la dinámica de los medios de comunicación y ofrecía gratuitamente sus servicios a otros Anons. En el curso de una entrevista, un Anon que trabajaba en la redacción de notas de prensa lo explicó de esta manera: «Fue Barrett quien me enseñó cómo llamar la atención de los periodistas, cómo conseguir que se publicaran [las notas de prensa], cómo utilizar el ciclo de las noticias y escoger el momento oportuno y esa clase de cosas.» Finalmente, sus travesuras y el hecho de que asumiera el papel de agente de prensa no sentaron muy bien a la ética

dominante en Anonymous. AnonOps proscribió informalmente a su propio bufón de corte.

No se tolera la promoción personal

A mediados de diciembre de 2010, el periodista del *The Washington Post* Ian Shapira se puso en contacto conmigo. Le proporcioné información sobre la historia de Anonymous y le animé encarecidamente a hacer una visita al IRC, específicamente al canal #reporter, para el artículo en el que estaba trabajando. No estoy segura de si lo hizo alguna vez, pero el 22 de enero de 2011, Shapira publicó un artículo fundamental en el que presentó a un participante de AnonOps que actuaba en el área de Washington:

> Se le conoce con el nombre en clave de AnonSnapple para mantener en secreto el hecho de que forma parte del colectivo de ciberbromistas y activistas de Internet llamado Anonymous. Son muy pocas las personas de su escuela privada en el D.C. que saben que ese estudiante de 17 años del último curso asiste a las protestas públicas convocadas por Anonymous, donde lleva la máscara del sonriente y bigotudo Guy Fawkes que representa al movimiento.
>
> A AnonSnapple, que vive cerca de Bethesda con su madre, ama de casa, y su padre, economista en el Fondo Monetario Internacional, le preocupa que los investigadores puedan vincularle con los ataques de DDoS lanzados el mes pasado por parte de algunos miembros de Anonymous contra MasterCard, Visa y PayPal, que habían dejado de procesar los pagos efectuados a WikiLeaks. «Hace algún tiempo, el FBI llevó a cabo redadas a servidores de Anons que estaban implicados en esos ataques», dijo. «Aunque yo no participé en la acción, sigo formando parte de ellos. Sigo teniendo una presencia activa en las mismas salas de chat que las personas que [realizaron] los [ataques] DDoS... Me pueden relacionar fácilmente con ellos.»[149]

El 25 de enero de 2011, pocos días después de que se publicara el artículo, busqué el enlace en #reporter. Antes de hacerlo, el canal mostraba la

frenética actividad habitual, saturado de charlas. A los pocos minutos de salir el artículo, todo estalló. Estuve cerca de una hora investigando en diferentes canales de IRC, principalmente en #reporter y #lounge:

<shitstorm>: parece que snapple hizo esto sin ayuda
<shitstorm>: por ejemplo una entrevista local
<biella>: traté de encontrarle en irc pero creo que nunca lo consiguió y bueno se le ve el plumero
<shitstorm>: Esa entrevista es ridícula, además de un anuncio para snapple
<shitstorm>: es puro "namefagging"
<shitstorm>: Yo hice esto
<shitstorm>: Yo hice aquello
<owen>: así es
<q>: :/
<shitstorm>: Es de retrasados realmente
<shitstorm>: Me vuelve loco
<owen>: le eliminaré
<owen>: de todas partes
<shitstorm>: excelente
<owen>: una estupidez interesada
<shitstorm>: "Le preocupa mucho que puedan vincularlo"
<shitstorm>: ENTONCES NO OFREZCAS TODOS ESOS DETALLES

Al observar la conversación que inundaba mi pantalla podía sentir el furioso desprecio que emanaba de aquellas palabras. Escocía. Aunque entendía el origen de su ira, para entonces había trabajado con suficientes periodistas como para ofrecer el siguiente consejo preventivo:

<biella>: antes de eliminarle hay que asegurarse de que el periodista no estaba tergiversando nada (a menos que se trate de un patrón)
<owen>: estoy tan harto de los críos que creen que esto es una especie de juego gigante
<q>: debe de haberlo tergiversado todo
<biella>: pero quién sabe, acaban de tergiversar mis palabras muy, muy, muy gravemente
<q>: y no creo que ian sea capaz de hacer eso
<q>: es un periodista serio
<owen>: eso suena exactamente a snapple en mi opinión
<shitstorm>: estoy de acuerdo
<biella>: bien, seguro que todos vosotros sabéis más que yo

Aunque en ocasiones los Anons trabajaban seriamente con periodistas, con frecuencia también los troceaban o troleaban (sí, incluso a los “periodistas serios”). Pero ésta no era una de esas ocasiones. Lo que más enfadó a la gente fue la forma en que AnonSnapple, que no había corrido ningún riesgo personal durante ninguna operación, hablaba en nombre de quienes sí habían corrido riesgos:

<owen>: no sabe nada

<owen>: necesita gtfo [irse a tomar por el puto culo]

<owen>: ¿no es uno de los vuestros, q?

<shitstorm>: AnonSnapple le preguntó hace poco a un profesor si podía presentar una hoja de asistencia con las horas que había pasado diseñando y distribuyendo folletos para una manifestación de Anonymous en Dupont Circle.

<shitstorm>: ¿ME TOMAS EL PELO?

<shitstorm>: !!!!!!!!!!!!!!!!1

<shitstorm>: !poner la furia a tope

<owen>: quiero saber cuando aparece por favor

<owen>: estúpidos críos gamberros

<shitstorm>: no, voy a estrangularlo

<shitstorm>: también

Y estrangularlo fue prácticamente lo que hicieron a continuación. Citaron a AnonSnapple en el canal:

<shitstorm>: por dios Snapple

<shitstorm>: qué es esto

<shitstorm>: ?

<shitstorm>: Snapple que debe ser el mierda más imbécil, más imbécil que cloldblood

<shitstorm>: coldblood*

<q>: ahora está conectado.

<owen>: snapple

<owen>: habla ahora

<shitstorm>: Snapple

<shitstorm>: Snapple

<owen>: antes de que te quite de aquí

<shitstorm>: Snapple

<Nessuno>: Snapple es un marica

<Nessuno>: silencioso
<shitstorm>: porque sabe que está acabado
<Snapple>: jajaja
<shitstorm>: oh, hola
<Snapple>: os creéis que la mitad de esa mierda es verdad
<MTBC>: porque sabe que está jodido
<owen>: ¿crees que es divertido?
[...]
<shitstorm>: Snapple, ¿por qué no lo sería?
<owen>: así que espera
<shitstorm>: parece cierto por lo que he oído y visto
<owen>: ¿estás diciendo que mintieron?
<owen>: LES TRAERÉ AQUÍ AHORA MISMO
<Snapple>: Porque nunca diría dónde vivo
<owen>: y veremos
<Snapple>: En primer lugar
<Snapple>: ni lo que hacen mis padres
<shitstorm>: bueno nos dices que estás en dc
<owen>: lo harías si buscaras la gloria
<Snapple>: vivo en DC
<shitstorm>: derp [abreviatura de derptrolling, grupo de hackers]
<Snapple>: Eso es todo
<owen>: todos sabemos dónde vives
<shitstorm>: ^
<Snapple>: :)
<owen>: se lo dices a todo el mundo
<Snapple>: ven a visitarme
<shitstorm>: muy bien
shitstorm coge la escopeta
<shitstorm>: owen, ¿vamos, de acuerdo?
<Snapple>: ***runs***
<shitstorm>: Master-IT trae el M16
MTBC roba la escopeta y se dispara en la cara Snapple abandona la habitación (quit: Z:lined (gilipollas)).

La furia contra AnonSnapple era tan profunda e intensa que incluso la prohibición —habitualmente un eficaz mecanismo de liberación— apenas si consiguió disipar los oscuros nubarrones. Los Anons aún estaban furiosos y lanzaban un diluvio de insultos —owen, por ejemplo, anunció que «mientras tanto, snapple puede concentrarse en sus deberes del cole en

lugar de visitar el IRC esta noche». Cuando les informé que conocía al periodista, me pusieron a trabajar:

<biella>: owen, q, conozco a ian
<q>: era periodista
<q>: biella, ¿podrías ayudarnos en este asunto?
<biella>: claro, podría contactar con él o hacerle saber que debería ponerse en contacto con q

Finalmente, en otro canal, owen añadió algunas observaciones finales:

<owen>: tratar de poner todo el trabajo que han hecho tantas personas al servicio de tu promoción personal es algo que no pienso tolerar
<Nessuno>: lo que dice owen es razonable
<owen>: él era todo 'eh miradme pero yo no he hecho nada'
<butts>: No puedo creer que le haya contado todo esto
<owen>: no

INSULTAR LA CARNE

Estaba estupefacta. Desde luego, estaba familiarizada con la prohibición del "namefagging", que consiste en vincular tu identidad a tus acciones. La norma estaba tan bien establecida en Anonymous, remontándose incluso a sus días preactivistas, que raramente se vulneraba, al menos en aquellos días (aunque pronto acusarían a Barrett Brown de semejante conducta). Pero nunca había visto las repercusiones en tiempo real. El detalle que lo volvía todo más fascinante era que finalmente había podido ser testigo de un fenómeno del que antes solo había leído en los relatos etnográficos. Las tácticas destinadas a reforzar el ideal del igualitarismo son muy comunes, pero varían en cuanto a su carácter moral en las distintas culturas. Estas tácticas incluyen desde arruinarle la vida a alguien (como denunciar que es una bruja) hasta otras relativamente mundanas, pero todas muy eficaces. Uno de mis ejemplos favoritos procede del pueblo !Kung, que habita en el desierto del Kalahari, en África. Entre los !Kung, a los cazadores que regresan a la aldea con un enorme trozo de carne, no los cubren de elogios, como se podría esperar de una tribu que ama la carne, sino de insultos. Las

burlas ayudan a mantener los egos bajo control:

> «Pongamos que hay un bosquimano que ha estado cazando. Nunca debe regresar a casa y anunciar como un fanfarrón, '¡He matado un animal grande en el bosque!' Primero debe sentarse en silencio hasta que yo o alguien se acerque a su hoguera y le pregunte, '¿Qué has visto hoy?' Él contestará tranquilamente, 'Ah, no soy bueno para la caza. No vi nada de nada [pausa], solo un animal muy pequeño.' Entonces yo sonrío para mí—prosiguió Gaugo—, porque sé que ha matado algo grande.
>
> »A la mañana formamos un grupo de cuatro o cinco personas para cortar y llevar la carne al campamento. Cuando llegamos a la pieza, la examinamos y gritamos, '¿Quieres decir que nos has arrastrado hasta aquí para que nos llevemos a casa tu montón de huesos? Oh, si hubiera sabido que era tan poca cosa no habría venido'. Otro de ellos dice, 'Gente, pensad que renuncié a un día agradable en la sombra para esto. Es posible que en casa tengamos hambre, pero al menos tenemos agua fresca para beber'.»[150]

La nivelación moral de esta naturaleza no elimina las relaciones de poder, y mucho menos las diferencias en cuanto a las capacidades. Algunos individuos son simplemente mejores cazadores que otros. En el IRC están aquellos, como owen y shitstorm, que dirigen la red y controlan inequívocamente la autoridad para aplicar normas recurriendo al poder técnico. Excluir a los individuos del IRC después de cubrirlos de insultos es una actitud que no genera precisamente igualdad. Este comportamiento solo es eficaz para minimizar y modular las diferencias de poder. Aunque en Anons es aceptable mostrar cierto grado de alabanzas, cualquier intento evidente de convertir el estatus interno en estatus externo se considera inaceptable. La persona pública, individual, debe permanecer fuera de la ecuación, en interés de la fama colectiva.

Si AnonSnapple hubiese alcanzado logros más importantes —especialmente la arriesgada tarea de la desobediencia civil— sospecho que habría recibido un castigo que no implicase el destierro. Al reclamar la suficiente responsabilidad como para ser retratado al tiempo que ofendía las

arriesgadas acciones llevadas a cabo por otros, la actitud de engrandecimiento de AnonSnapple fue recibida como una afrenta de orden superior. Para entonces la gente estaba más que enterada de los riesgos jurídicos (solo dos años más tarde comenzaron las detenciones en el Reino Unido y se dictaron órdenes de arresto en Estados Unidos como respuesta a la reciente campaña de ataques de DDoS). Se consideró que AnonSnapple había actuado impulsado por un incorrecto interés propio, y las docenas de tíos que se conectaron a #lounge contemplaron su exterminio con una bolsa de palomitas en la mano. Pero no se trataba de un mero entretenimiento. Esta paliza sirvió de clara lección moral para un público más amplio, que avaló tácitamente la decisión con su silencio o su eventual conformidad.

«El susto de los nerd»

El mismo día del destierro de Snapple regresó mi viejo vértigo debido a una notable avalancha de acontecimientos que entraban y salían de AnonOps. A lo largo de las dos semanas siguientes me mantuve conectada todas mis horas de vigilia, observando cómo Anonymous participaba en una revolución histórica. Al tiempo que aceptaban la primera oleada de detenciones que hizo impacto en su red, planearon y llevaron a cabo el acto de venganza más extraordinario ejecutado por Anonymous.

El día en que AnonSnapple había sido convocado sin miramientos a comparecer en el monte Olimpo y expulsado ritualmente, la Secretaria de Estado, Hillary Clinton, hizo pública una respuesta a la creciente sublevación popular que se desarrollaba en Egipto: «Nuestra evaluación es que el gobierno de Egipto es estable y está buscando vías para responder a los intereses y necesidades legítimos del pueblo egipcio.»[151] Los egipcios, que seguían la estela del fermento revolucionario de Túnez, se manifestaron en las calles durante la mayor parte de enero para exigir la dimisión de Muhammad Hosni El Sayed Mubarak, el dictador que llevaba tres décadas en el poder. Los organizadores egipcios habían convocado un día de protesta el 25 de ese mes y una multitud de manifestantes respondió a la llamada. A medida que se desarrollaban los acontecimientos, el recién bautizado canal público #OpEgypt se vio invadido por la excitación y el horror (los seudónimos se han cambiado):

<WebA18>: si, censuran twitter en egipto
<WebA18>: y están tratando de censurar facebook
<0n>: los teléfonos móviles también
<t23>: al no estar en egipto no puedo confirmarlo al 100%
<0n>: LA HORA DEL PÁNICO
<t23>: pero es una táctica conocida
<WebA18>: un amigo en egipto me dice que lo han censurado
<eb>: Ps, si estáis cerca, plantearos manifestaros ante la embajada de egipto
<Ion>: ÚNETE A #propaganda PARA CREAR Y DISEÑAR MATERIAL PARA #opegypt
<jeb>: para conseguir la atención de los medios y apoyo para nuestros /b/hermanos egipcios
[...]
<WebA18>: ¡gracias!
<mib>: Las protestas se extienden y aumentan en número
<bi>: Los egipcios tienen las pelotas de acero. ¡VAMOS, VAMOS, VAMOS!
<pi>: ¿hay alguna fuente colectiva a la que deba conectarme para participar?
<mib>: no debemos detenernos hasta que este régimen haya caído Argelia: traducción: el gobierno ha bloqueado los teléfonos móviles
<b>: Difundir ese POSTER para RECLUTAR a más gente: http://i.imgur.com/LfLhN.png

Lo que al principio había sido un destello esporádico de interrupciones de las comunicaciones iniciadas por el gobierno, el 28 de enero se convirtió en una acción generalizada. El gobierno egipcio apagó toda la jodida Internet.

Con el propósito de restablecer alguna conectividad, Anonymous se unió a otro equipo hacktivista, Telecomix. AnonOps y Telecomix habían tenido diferencias en el pasado. Telecomix, opuesto a las tácticas de DDoS, intentaba mantener los sitios activos, mientras Anonymous trataba de ralentizar el acceso. Pero si hay un problema urgente o lo bastante interesante que resolver —como restablecer el acceso a las comunicaciones para la gente que lo necesita— los hackers pueden dejar de lado las diferencias importantes para trabajar codo con codo. Un grupo de Anons contribuyó a que el esfuerzo encabezado por Telecomix lograse averiguar de qué manera podían utilizarse los modems, faxes y teléfonos viejos para conectarse de manera enrevesada a Internet. Al mismo tiempo, la pequeña élite técnica de Anonymous, que se había unido durante OpTúnez para

crear un canal permanente de IRC, continuó con sus hackescapadas en apoyo a la Primavera árabe.

A medida que OpEgipto adquiría impulso contra el gobierno de Mubarak, el propio Anonymous se vio amenazado. Dos días después del destierro de Snapple y el día histórico de la ira egipcia, la siguiente advertencia destelló en #reporter con grandes letras rojas:

> <ew>: ATENCIÓN: ¡Cualquiera de vosotros anons que seáis de EEUU o Reino Unido y hayáis participado en los ataques a Mastercard, Visa o BOA [Banco de América], borrad cualquier dato de vuestras máquinas que pudiera relacionaros con ellos, ahora mismo!

El 27 de enero de 2011, las autoridades acorralaron y arrestaron a presuntos participantes en el Reino Unido, mientras que en los Estados Unidos tres agentes del FBI emitieron cuarenta órdenes de detención en relación con la campaña de ataques DDoS Operación Venganza llevada a cabo en diciembre de 2010 (y finalmente arrestaron a un grupo de catorce Anons conectados con estos ataques):

> <Anonymous9>: Eh colegas
> <Anonymous9>: supongo que todos habéis escuchado la noticia :(
> <shitstorm>: sí
> <shitstorm>: es un día triste en mi opinión
> <shitstorm>: un nuevo golpe de los gobiernos
> <Anonymous9>: Realmente triste
> <Anonymous9>: Pero, para ser justos, no inesperado.
> <shitstorm>: bueno, eso es verdad
> <Anonymous9>: Sí
> <shitstorm>: pero ellos siguen jodiendo a todo el mundo en busca de pruebas
> <Anonymous9>: Es increíble la forma en que nos están persiguiendo tan meticulosamente
> <Anonymous9>: Mientras los verdaderos criminales nombrados en los cables filtrados por wikileaks son defendidos por sus respectivos gobiernos
> <Anonymous9>: Hay algo muy enfermo en todo eso
> <shitstorm>: Estoy de acuerdo
> <Anonymous9>: Quiero decir, a pesar de lo que digan sobre nosotros nunca hemos participado en torturas ni asesinatos
> <Anonymous9>: Sin embargo están gastando lo que debe de ser un montón de pasta para que la gente vaya a por nosotros

<Anonymous9>: Mientras a todos aquellos que cometieron los delitos más graves les ofrecen inmunidad diplomática y toda esa mierda

Anonymous9 evaluó críticamente el primer ataque estatal importante contra Anonymous con un lamento incisivo y conmovedor sobre la hipocresía del poder del Estado. Desde aquella primera intervención de las autoridades gubernamentales, más de un centenar de personas ha sido arrestado en todo el mundo, desde Indonesia hasta la República Dominicana, desde Camboya hasta Estados Unidos. Estos arrestos son históricamente excepcionales, un listón muy alto en la historia del hackeo. Nunca antes un número tan grande de hackers y geeks había sido acorralado por sus ideas y acciones políticas en una sola ofensiva coordinada en todo el mundo. Durante las décadas de 1980, 1990 y 2000 se arrestó a un montón de hackers, pero los allanamientos eran más esporádicos y habitualmente asumían una de dos modalidades diferentes (excluyo a los hackers arrestados por operaciones puramente criminales, como el *carding* o uso fradulento de tarjetas bancarias):[152] la actuación policial buscaba a hackers individuales, como Kevin Mitnick o Gary McKinnon, que no se dedicaban a la piratería informática en nombre del cambio social, sino para su propio placer, o bien asaltaban a los grupos de hackers underground para desactivarlos y cerrar sus lugares de encuentro, tales como los sistemas de boletines electrónicos. La más famosa y amplia de estas actuaciones fue la llamada Operación Sundevil, que se llevó a cabo simultáneamente en catorce ciudades estadounidenses el 8 de mayo de 1990, cuando se ejecutaron veintisiete órdenes de búsqueda y se realizaron cuatro arrestos.[153] En algunas ocasiones, como ocurrió en el caso del joven Julian Assange, los hackers con habilidades para afrontar objetivos políticos más ambiciosos debieron hacer frente a cargos criminales, pero esta clase de intervención era menos común y los arrestos por estos motivos eran incluso más raros.

Con Anonymous llegó el primer movimiento hacktivista a gran escala que provocó una amplia y coordinada campaña multiestatal. Constituye lo que Gráinne O'Neill, en aquellos días representante del National Lawyers Guild de muchos de los arrestados, describió acertadamente como «el susto de los nerd».

¿QUIERE SENTARSE?

Después de haber conocido y entrevistado desde entonces a individuos incluidos en «el susto de los nerd», me quedó grabada la versión de los hechos ofrecida por una persona en particular, Mercedes Haefer. Haefer se unió a la red de AnonOps en noviembre de 2010, cuando tenía 19 años, y llegó a destacar rápidamente gracias a su inteligencia y ácido ingenio. Haefer es y era una fuerza lingüística de la naturaleza, su verborrea es capaz de torear a un marinero borracho que busca pelea. Estuve con ella formando parte de un panel durante la edición de 2012 de DEF CON, la conferencia de hackers más importante del mundo. Antes de entrar en una seria y apasionada descripción de su participación en Anonymous, exigió que el público presente —compuesto por aproximadamente un 99 por ciento de hombres— enseñara las tetas o se largara de allí («Tetas o te largas de una puta vez» es un comentario despectivo que, en algunas comunidades online, obedece a la autoidentificación de cualquier usuario como mujer).

DEF CON se celebraba en Las Vegas, donde resulta que vive Haefer. Sin embargo, su apartamento se encontraba en una zona muy alejada de la sede de la conferencia, de modo que le sugerí que se quedara en mi habitación del hotel, con una condición: que ese trol inimitable, el trol de todos los trols, weev, no pudiera ni acercarse a la habitación. Weev había estado tratando de ligar con ella a través de Twitter y alguien le había visto en la conferencia, y aunque me apetecía pasar un rato con él, y no me oponía de ninguna manera a su búsqueda de cualquier afecto mutuo, no podía soportar la idea de que un repugnante hijo del amor trol pudiera ser arrancado de las profundidades del infierno como resultado de un profano encuentro carnal en *mi* habitación de hotel (demasiada responsabilidad y sin las bastantes conexiones con exorcistas).

Mercedes estuvo de acuerdo y en Las Vegas nos enfrascamos en un montón de conversaciones que posteriormente continuaron en la red. Cuando supe que había sido víctima de una de las tristemente célebres operaciones gubernamentales llevadas a cabo en este período, le pregunté qué se sentía al tener al FBI encima. Vale la pena contar su historia porque tener una imagen mental de lo que sucede durante esos momentos es útil para negociar una visita potencial de los agentes de la autoridad. La mayoría de las personas que entrevisté no estaba preparada para hacer

frente a una súbita y amenazadora demostración de fuerza; son personas que hablaban libremente cuando deberían haberse quedado en silencio excepto para pedir un abogado. Como lo expresó el hacker Emmanuel Goldstein durante el famoso panel de HOPE sobre los chivatazos, «a la gente le entra el pánico, a la gente le entra el pánico... y la autoridades cuentan con eso. Las autoridades viven para esta clase de cosas y así consiguen la máxima información posible». (Señalar que el relato que sigue sobre el operativo es en gran medida anecdótico y representa su versión de la historia. Pero muchos de los detalles esenciales coinciden con las descripciones de hechos encontradas en el documento del FBI conocido como FD-302, un resumen de entrevistas que más tarde alguien me filtró.)

El FBI llegó al amanecer. Haefer dormía tranquilamente en su apartamento en un barrio de clase obrera de Las Vegas cuando entre cinco y ocho agentes se acercaron en silencio aquel amanecer de invierno en el desierto. (A Haefer le costaba recordar el número exacto de agentes ya que estaba desorientada. «Todos se parecían», explicó.) Rompieron el silencio aporreando la puerta de entrada. Aunque había sido arrancada del sueño, no sintió miedo, e imaginó simplemente que su padre, que trabajaba en horarios extraños, se había olvidado las llaves. Salió a rastras de la cama y se dirigió a la puerta en pijama, para ser recibida con «la luz de una linterna en la cara, algo que a las seis de la mañana le molesta a cualquiera». El carácter desconcertante de la situación aumentó al comprobar que un par de cañones de fusil también apuntaban en su dirección.

Describió cómo la sacaron por la puerta, la llevaron por la pasarela que atravesaba el complejo y luego comenzaron a cachearla. Mientras realizaban un exhaustivo registro no dejaban de hacerle preguntas, tratando de confirmar su identidad. Al comenzar el interrogatorio, su boca se despertó y contraatacó. «Soy yo, capullo. Que te den. Yo me vuelvo adentro. Hace frío.» Una vez cumplida esa formalidad, todos regresaron a la calidez de su apartamento.

Uno de los agentes le preguntó si quería sentarse. Ella cuestionó su sinceridad y percibió su gesto como un alarde de poder. «¡No le preguntas a alguien si quiere sentarse en su propia casa!», me explicó. Esa afirmación la llevó a una repentina toma de conciencia: «Estos tíos no son mis amigos. No me ayudarán. Están aquí para cumplir con su trabajo.»

Los agentes registraron la casa, tomaron fotografías del equipo,

confiscaron su ordenador y la interrogaron. Ella me había dicho que era un poco sabelotodo; la historia siguiente lo confirmó. Tal como dicta el protocolo oficial del FBI, dos de los agentes se emparejaron para llevar a cabo el interrogatorio, uno formulando las preguntas mientras el otro apuntaba las respuestas.[154] Afirma que le preguntaron por 4chan. En aquel momento, pensó, «si creéis que esto va de 4chan, es que sois mucho más incompetentes de lo que pensaba». Me contó que comenzó a parlotear «sobre ese hilo que había leído sobre un tío que estaba enamorado de su perra y quería que se quedara preñada, así que estuvo consiguiendo muestras, las revolvió en una taza, se las inyectó en el pene y la dejó preñada».

Ella advirtió que «al oír esta parte dejaron de tomar notas», y —con toda seguridad— no hay ninguna mención de 4chan en el relato filtrado presentado por los agentes. Pero, considerando el descaro de Haefer y su dominio del lulz, resulta teóricamente posible, incluso verosímil. Y la exclusión de ese comentario puede ser coherente con su metodología. El FBI (comprensiblemente) no está en la onda del lulz (mucho menos de documentarlo). Basándome en dos documentos adicionales que también me entregaron (que incluyen entrevistas con otros dos Anons a los que el FBI visitó el mismo día y que finalmente fueron arrestados), el género combina extensos resúmenes de entrevistas que se atienen a declaraciones objetivas con alguna cita directa ocasional, mientras pasan por alto las trivialidades. No hay ninguna constancia, ni mucho menos reflexión, sobre el tono o el contenido emocional del intercambio.

Y sin embargo, en el relato de los hechos que me hace Haefer, estos pequeños actos de desafío tienen un significado importante. En ese intercambio, los agentes de la ley y Haefer aplicaban criterios muy diferentes cuando se trataba de evaluar la información, tal como cabría esperar en una situación de esa naturaleza. Independientemente de si eran troleados, o eran conscientes de que estaban siendo troleados, o de si les preocupaba en cualquiera de los dos casos (o si me estaban troleando a mí), el informe de los agentes se atiene a cuestiones de interés jurídico.[155] Los agentes escribieron: «Luego Haefer preguntó cuál era el propósito específico de la búsqueda y el interrogatorio. Luego el agente especial (AE) X le dijo a Haefer que creía que ella (Haefer) ya conocía la razón por la que el FBI estaba registrando su casa y del interrogatorio. Ella entonces

respondió que ellos estaban allí por “DDoSeo y vandalismo”.»

Aun así, el informe del FBI y el relato de Haefer coinciden en muchos aspectos. Le pidieron varias veces que «explicara más» y ella respondió haciendo referencia a una variedad de cuestiones: desde su participación concreta en diversas actividades hasta reflexiones más extensas sobre la ética del DDoSeo. Al principio, el informe la registra afirmando que ella «no estaba tan implicada en ninguna de las dos actividades [vandalismo o DDoS]» pero «después de decirle que no estaba siendo sincera» (demostrado, según le dijeron, por pruebas encontradas en los archivos de IRC), admitió que tenía pleno conocimiento de que su ordenador estaba implicado en los ataques de DDoS a PayPal y que ayudó a otros a configurar la aplicación LOIC. También les entregó todos sus nombres de usuario, cuya lista incluye el informe, pero afirmó no recordar los nombres de las salas de chat, operadores y servidores porque eran demasiados (en otros informes que he leído, los interrogados tuvieron menos dificultades para recordar esos nombres).

El informe de Haefer, así como el de los otros dos a los que tuve acceso, intenta describir, en alguna medida limitada, las defensas políticas presentadas por participar en campañas de DDoS. Pero la presentación de esta información era diferente según procediera de Haefer o del informe. Ella me dijo que le preguntaron directamente sobre Assange. Esa pregunta no constaba en el informe, sino solo la siguiente declaración que, no obstante, resulta interesante: «Ella apoyó que PayPal fuese un objetivo de DDoS porque no le gustaba que PayPal retuviera la cuenta de Julian Assange, era dinero que le debían a Assange [*sic*]. Recalcó que no era fan de Assange, que solo estaba disgustada por lo que PayPal había hecho.» Esto se incluyó además de un resumen detallado de su defensa política:

> Haefer estaba de acuerdo con lo que hace Anonymous. Cuando una empresa o un negocio en el mundo real está haciendo algo inaceptable, se puede protestar delante de su sede. Puesto que VISA o Mastercard funcionan online, no se puede protestar físicamente contra ellas y, por lo tanto, deben ser protestas en línea, o en forma de ataque DDoS. Haefer describió esas protestas como un “derecho”.

Durante nuestra entrevista me explicó lo que quería decir con “derecho”:

> Se trataba de derechos. No se trataba de mostrar apoyo a Assange. Se trataba de defender la libertad de expresión y la transparencia del gobierno. Se trataba de decirle al gobierno que no podían simplemente interferir en casos judiciales en el extranjero. Se trataba de decirle al gobierno que trabaja para nosotros y no a la inversa. Y aunque a mí no me gustaba Assange, seguía creyendo que él tenía derecho a la libertad de expresión y a un juicio justo. Y que si solamente apoyamos los derechos de las personas que nos gustan, entonces no son derechos sino privilegios. Y que los privilegios pueden quitarse. Los derechos no pueden quitarse. Solo pueden ser oprimidos.

Para el FBI es habitual aparecer a las seis de la mañana, y también es habitual pedirle a la gente que colabore. Esto puede significar varias cosas, desde suministrar información en el acto hasta convertirse en informador. Haefer afirma que se lo pidieron (y esta solicitud también constaba en los otros dos informes completos que cayeron en mis manos). Ella lo rechazó o, en sus propias palabras, más elocuentes, «los mandé a la mierda».

Cuando el agente especial se marchó, Haefer sintió que, a pesar de todo lo que ella acababa de decirle, él seguía considerándola una trol delincuente en lugar de una activista. Según la versión de Mercedes, le entregó su tarjeta y le pidió que «por favor no fuera a por su familia». «Si él aún pensaba que eso era un problema, entonces todavía no había entendido el caso», dijo ella. Pero no conocemos la versión del agente del FBI, quizás también él le estaba gastando una broma pesada.

Al reflexionar sobre la situación, Haefer, que, como tantos Anons, fue sorprendida con la guardia baja cuando los federales llegaron a su casa, concluyó: «Si volvieran a allanar mi casa, probablemente no les diría que lo hice.» Pero entonces, igual que ahora, se sentía orgullosa de su pequeña contribución a la defensa de los derechos.

Cómo protestar de forma inteligente

Docenas de personas en Estados Unidos fueron interrogadas con el mismo método durante ese período. Algunas compartieron sus relatos entre ellas o participando en diversos foros poco después de ocurridos los hechos, pero

en general ninguna tenía una idea precisa de lo que había sucedido. Mientras tanto, Anonymous continuaba contribuyendo al duro trabajo de derrocar a un régimen. Miles de egipcios bajaban a la plaza Tahrir, o plaza de la Liberación, en la primera de las ocupaciones dinámicas que finalmente tendrían lugar en España, luego en Norteamérica y, finalmente, en el resto de Europa. Las cifras eran apabullantes. El 31 de enero, la plaza congregó a 250.000 personas. Pero el ambiente de emocionado entusiasmo se vio empañado por una escalada de violencia. En los canales de IRC, muchos egipcios pedían que Anonymous atacara al gobierno y a los medios de comunicación controlados por el Estado. El colectivo se negó. Si bien algunos grupos estaban realizando ataques de DDoS contra sitios web del gobierno —una acción que molestó a Telecomix— el consenso general, que encontró eco en los chats de IRC y en declaraciones públicas, era que nunca se debía atacar a la prensa (se han cambiado todos los seudónimos):

> <dr>: hola, como egipcio pido que ataquéis a sus medios de comunicación ¡por favor!!! http://www.ahram.org.eg/ "http://www.algomhuria.net.eg/"http://www.algomhuria.net.eg/
> <MS>: http://ahram.org.eg/ <--- el principal periódico solo ha estado hablando del líbano
> <sudor>: ¡tíos confiad en mí! es mucho más útil acabar con AHRAM. ORG.EG
> <Fr>: a los medios no
> <hat>: sudo, yo argumenté eso pero va contra nuestra política atacar a un medio de comunicación, aunque sea propiedad de un régimen dictatorial
> <at>: sudo, ¿el medio del que estás hablando es parte del gobierno?
> <sudor>: ¡SI LO ES at!
> <tru>: a los medios no
> <kan>: tíos, Egipto os Ama y reza por vosotros
> <Ter>: A LOS MEDIOS NO
> <Cyberp>: lrn2protect libertad de expresión
> <MS>: ahram es un medio de comunicación engañoso
> <Ci>: Junto con MCIT
> <cru>: Gracias, kanta.
> <sudor>: ahram es propiedad del gobierno
> <Cyberp>: los medios engañosos también son medios

Como parte de su trabajo, Anons de AnonOps, miembros de marblecake y de Telecomix, crearon un panfleto sorprendentemente detallado y bien

ilustrado con el título “Cómo protestar de forma inteligente”.

Hacia final de mes era como si AnonOps estuviera actuando más como un organismo defensor de los derechos humanos que como una manada de trols borrachos de lulz. Sus esfuerzos se alejaban de las acciones unilaterales hacia el apoyo infraestructural que podría permitir que los ciudadanos esquivasen a los censores y la vigilancia electrónica. Ellos enviaron un paquete de asistencia compuesto de herramientas de seguridad, consejos tácticos y ánimos, como esta nota, que clarifica el limitado papel que cumplen los medios sociales en esos levantamientos, incluso si están pregonados por los expertos como una “Revolución en Twitter”: «Ésta es *vuestra* revolución. No será tuiteada ni televisada o trasmitida por IRC. *Debéis* salir a las calles o *perderéis* la batalla.»

Mientras muchos Anons se sentían estimulados por su capacidad para apoyar el histórico derrocamiento de regímenes dictatoriales en Oriente Medio, para otros no podía haber una prueba más evidente de la supremacía de la moralfaggotry. De hecho, con su contribución a las revoluciones árabes y sus idealistas fines políticos, Anonymous se había transformado de tal manera que parecía como si, al igual que en el caso de AnonSnapple, el propio lulz se hubiese desterrado a sí mismo. Al final, éste no fue el caso. Mientras las revoluciones bramaban en el extranjero, un pequeño grupo de hackers tomó represalias contra un investigador de seguridad estadounidense y su empresa y el lulz regresó con la venganza bajo el brazo.

Capítulo 7

La venganza del Lulz

Algunas de las características básicas de la cultura política nacidas del anonimato no son ni nuevas ni difíciles de entender. Analicemos la filtración anónima que reveló la existencia de COINTELPRO, un programa de espionaje sistemático e ilegal a la población estadounidense. Una noche de 1971 en Pensilvania, un grupo autodenominado “Comisión de ciudadanos para investigar al FBI” accedió a una oficina del FBI utilizando una palanqueta para forzar la puerta. Mientras millones de estadounidenses sintonizaban sus aparatos de radio para escuchar las alternativas del enfrentamiento de Muhammad Ali con Joe Frazier en un épico combate a quince asaltos, los activistas vaciaban los archivadores de más de un millar de documentos. Aquellos documentos, relacionados con la cuestión de la vigilancia política, fueron filtrados a los medios de comunicación y publicados en el número de marzo de 1972 de la revista *WIN Magazine*, una publicación de la War Resisters League, y COINTELPRO quedó expuesto a la opinión pública por primera vez. El programa había sido iniciado en 1956 por el director del FBI J. Edgar Hoover, y funcionó con éxito hasta 1971.

Al principio, la misión de COINTELPRO era limitada: perturbar las operaciones internas del Partido Comunista de los Estados Unidos, que Hoover estaba convencido se encontraba bajo la influencia directa de infiltrados rusos. Pero su campo de acción se extendió rápidamente para incluir la interrupción del activismo político nacional en todas sus variantes, incluidas las iniciativas radicales, conservadoras e incluso las liberales moderadas. Uno de sus objetivos manifiestos era

> impedir el ascenso de un “mesías” que pudiera unir e impulsar el movimiento nacionalista militante negro. Malcolm X podría haber sido ese “mesías”; hoy es el mártir del movimiento. Martin Luther King, Stokely Carmichael y Elijah Muhammed aspiran a ocupar su puesto... King podría ser un serio competidor para este puesto si abandonara su

supuesta "obediencia" a las "doctrinas liberales blancas" (no violencia) y abrazara el nacionalismo negro.[156]

Y, de hecho, los documentos aportan pruebas claras de las elaboradas medidas que tomó el FBI para vigilar a King en particular. La vigilancia ilegal se prolongó durante años, con su punto de partida a finales de la década de 1950, cuando el programa recibió el visto bueno de Hoover. El 28 de agosto de 1963, cuando King pronunció su famoso discurso "Tengo un sueño" durante la Marcha sobre Washington, William Cornelius Sullivan, director asociado del FBI, escribió a Hoover, «debemos señalarlo [a King] ahora, si no lo hemos hecho antes, como el negro más peligroso para el futuro de esta nación desde el punto de vista del comunismo, la cuestión negra y la seguridad nacional». King estaba considerado como "un hombre sin principios" que tenía "el carácter débil". Sullivan escribió, «cuando sea el momento apropiado y pueda hacerse sin que resulte embarazoso para el Bureau, expondremos a King como un oportunista inmoral que no es una persona sincera sino que está explotando la situación racial en beneficio propio». Poco después de que King fuese nombrado "Hombre del Año" por la revista *Time*, el FBI fue autorizado ilegalmente para instalar escuchas en la habitación de su hotel; «la invasión de la propiedad está involucrada», escribieron. Las transcripciones resultantes se llevaron ante Hoover, que comentó, «esto destruirá a ese cabeza de erizo» (forma despectiva de referirse a los afroamericanos debido a su pelo notablemente rizado). Los micrófonos ocultos captaron pruebas de la infidelidad matrimonial de King, un hecho que entusiasmó a Sullivan y a Hoover, pues esas grabaciones se podían utilizar para destruir al "animal".[157] Un extracto de la carta enviada por el FBI para chantajear a King evidencia la abominable verdad histórica de que el gobierno de Estados Unidos aterrorizó a uno de los cruzados por las libertades civiles más venerado y pacífico de la nación:

King, solo hay una cosa que usted puede hacer. Y sabe lo que es. Tiene solamente 34 días para hacerla (este número exacto ha sido elegido para una persona específica, tiene un significado práctico definido). Está acabado. Existe una sola salida para usted. Será mejor que la tome antes de que su sucia, anormal y fraudulenta persona sea descubierta

ante la nación.[158]

El gobierno atacó de la misma manera a muchos otros grupos: Estudiantes por una Sociedad Democrática, supremacistas blancos, ramas del movimiento feminista, el movimiento radical independentista de Puerto Rico, e innumerables asociaciones contrarias a la guerra de Vietnam. Sus métodos agresivos y multidimensionales incluían estrategias de infiltración depredadora con el propósito de cometer actos de sabotaje: una perturbación sostenida, planificada y organizada de los movimientos políticos para acabar con ellos. El FBI sembraba información falsa, chantajeaba a los activistas, les llevaba ante los tribunales por incidentes relacionados con los impuestos y, en ocasiones, incluso recurría a la violencia física. Las órdenes insensatas de los agentes del gobierno les llevaban a alimentar a los medios de comunicación con historias falsas y a falsificar la correspondencia en representación de los grupos perseguidos. Parte del daño más duradero provino de agentes tan profundamente infiltrados en algunos movimientos que sus acciones erosionaron por completo los fundamentos de confianza sobre los que estaban construidos. Los agentes de COINTELPRO fomentaron un clima de miedo y desánimo, consumiendo la vitalidad de lo que habían sido yacimientos legítimos y profundos de actividad política.

Después de que las filtraciones de Ciudadanos llegaran a la prensa, siguieron otras intervenciones, incluida la publicación de documentos de COINTELPRO obtenidos a través de una petición que invocaba la Ley de Libertad de Información; Carl Stern, periodista de la NBC, utilizó estos documentos como base para su laureado reportaje sobre este tema. Una vez que se conoció en toda su amplitud la manipulación realizada por COINTELPRO de la discrepancia política legítima, legal e incluso la absolutamente común, la opinión pública se indignó. En las cámaras del gobierno estadounidense, un pequeño grupo de senadores constituyó en 1975 el Comité Church. Acabada la investigación, su conclusión fue inequívoca y firme en su acusación al programa: «Muchas de las técnicas empleadas serían intolerables en una sociedad democrática aun cuando todos los objetivos hubiesen estado implicados en actividades violentas, pero COINTELPRO fue mucho más allá de eso... El Bureau llevó a cabo una sofisticada operación de *vigilante*.» (cursiva de la autora).[159] A ello

siguieron numerosas reformas, incluida la limitación del mandato a un único período de diez años.

Poco después de obtener los archivos, la Comisión de Ciudadanos envió las filtraciones a la prensa junto con un comunicado que querían que se incluyera en todas las nuevas noticias relacionadas con los documentos del FBI. El comunicado explicaba sus motivos y objetivos:

> Deseamos que estos documentos tengan la mayor difusión para que puedan utilizarse eficazmente por todos aquellos que trabajan para conseguir una sociedad más abierta, justa y pacífica. Nuestra intención no es solo corregir las infracciones más flagrantes de los derechos constitucionales por parte del FBI dentro del marco de su organización y sus objetivos actuales. No es tampoco atacar personalmente a informantes, agentes o administradores. Nuestro propósito es, en cambio, contribuir al movimiento en favor de un cambio constructivo fundamental en nuestra sociedad, ya que como hemos manifestado en nuestra declaración inicial, «mientras un gran poder económico y político permanezca concentrado en manos de pequeñas camarillas no sujetas al control y el escrutinio democráticos, debemos esperar represión, intimidación y detenciones».[160]

Aunque sus intenciones se hicieron públicas, los propios miembros de la organización permanecieron en el anonimato hasta enero de 2014, cuando un puñado de ellos decidió dar un paso al frente.[161] Con el fin de revelar estas tácticas tóxicas, los activistas infringieron la ley y utilizaron el anonimato para protegerse de las consecuencias derivadas de sus acciones. Esta exposición dramática no se produjo online; no hubo máscaras de Guy Fawkes, no se abrieron ventanas de diálogo, no hubo correos electrónicos en *pastebins* (aplicación web que permite que los usuarios suban pequeños textos para que estén visibles para el público en general) y WikiLeaks no cumplía ninguna función. Pero el concepto era el mismo: encubrir la identidad para protegerla, para desviar la atención de los mensajeros y conseguir divulgar el mensaje incriminatorio. Si no hubiera sido por el robo de documentos ocultos en archivadores y cajones de escritorio cometido por la Comisión de Ciudadanos para Investigar al FBI, COINTELPRO probablemente habría seguido activo, dejando a su paso un rastro de

destrucción todavía más repugnante.

Avancemos rápidamente hasta el 5 de febrero de 2011, cuando Anonymous destapó una conspiración empresarial diseñada por la empresa de seguridad HBGary Federal, con sede en Washington, DC, para espiar y dificultar las acciones de WikiLeaks. Dada la naturaleza digital de los documentos contemporáneos ya no hay ninguna necesidad de abandonar la comodidad del hogar, y mucho menos de irrumpir en una oficina, para acceder a documentos secretos. Trabajando juntos en el IRC, los hackers de Anonymous entraron en el sistema informático de HBGary y descargaron setenta mil correos electrónicos de la empresa junto con otros archivos que incluían una presentación en PowerPoint titulada "La amenaza de WikiLeaks". Las tácticas sugeridas en ese documento son sorprendentemente similares a las practicadas y perfeccionadas durante la aplicación del programa COINTELPRO. La presentación describe un conjunto de estrategias que la empresa afirmaba que podían ser "desplegadas mañana":

Palantir Tácticas Proactivas Potenciales

- Alimentar el conflicto entre los grupos en disputa. Desinformación. Crear mensajes alrededor de acciones para sabotear o desacreditar a la organización contraria. Presentar documentos falsos y luego denunciar el error.
- Crear preocupación sobre la seguridad de la infraestructura. Crear noticias que le den visibilidad. Si el proceso se considera no seguro, estarán acabados.
- Ciberataques contra la infraestructura para conseguir datos sobre los remitentes de documentos. Esto acabará con el proyecto. Puesto que ahora los servidores están en Suecia y Francia, reunir un equipo para conseguir acceso es un método más directo.
- Campaña en los medios de comunicación para promover la naturaleza radical y temeraria de las actividades que lleva a cabo WikiLeaks. Presión sostenida. No consigue nada con los fanáticos pero crea preocupación y duda entre los moderados.
- Buscar filtraciones. Utilizar las redes sociales para retratar e identificar la conducta peligrosa de los empleados.

También proponían identificar e intimidar a los donantes de WikiLeaks y

manchar la reputación de simpatizantes y periodistas como Glenn Greenwald. Explicaron que estas personas eran «profesionales establecidos que tienen una tendencia progresista pero que, en última instancia, si a la mayoría de ellos se les presiona escogerán preservar su profesión antes que la causa; tal es la mentalidad de la mayoría de los profesionales de negocios».

Si bien Anonymous comprometió de manera ilegal los servidores para robar estos documentos, es probable que las acciones propuestas en la presentación PowerPoint, en caso de que se hubiesen concretado, habrían vulnerado un número todavía mayor de leyes. Tal como lo explica Glenn Greenwald: «Elaborar y presentar documentos falsos con la intención de que sean publicados es una acción que probablemente constituye falsificación y fraude. Amenazar las carreras de periodistas y activistas con el propósito de obligarles a guardar silencio es posiblemente extorsión. Atacar la infraestructura informática de WikiLeaks en un intento de comprometer sus fuentes viola sin ninguna duda numerosas leyes sobre el ciberespacio.»[162]

Mientras que la presentación "La amenaza de WikiLeaks" es similar en espíritu a COINTELPRO, existen también muchas e importantes diferencias. HBGary no es una agencia de inteligencia del gobierno, sino una empresa privada que había elaborado un plan para clientes privados. HBGary Federal, trabajando junto con otras dos empresas de seguridad, Palantir Technologies y Berico Technologies, estaba presentando la propuesta de sabotaje contra WikiLeaks al Bank of America a través de sus representantes legales en el bufete de abogados Hunton & Williams. Palantir y Berico, trabajando juntos bajo el nombre de Equipo Themis (una clara referencia a los antiguos titanes divinos griegos del orden y la justicia), esperaban que esas presentaciones dieran como resultado un lucrativo contrato. Assange había anunciado el 29 de noviembre de 2010 que tenía en su poder documentos que revelaban la existencia de un «ecosistema de corrupción [que] podía acabar con uno o dos bancos» y el Bank of America tenía razones para creer que era uno de esos bancos. Según *The New York Times*, el banco se puso manos a la obra, «registrando miles de documentos en el caso de que se hicieran públicos» y contratando a empresas de seguridad y bufetes de abogados externos «para ayudar a gestionar la revisión».[163] Teniendo en cuenta que el Bank of America no

fue citado directamente por Assange, su reacción tuvo el interesante efecto de llamar la atención sobre esa institución financiera.

Después de la filtración de documentos de HBGary, el Bank of America negó conocer la propuesta del Equipo Themis, describiéndola como "abominable", si bien estaba elaborada a la atención de uno de sus equipos jurídicos (el bufete Hunton & Williams nunca se pronunció sobre este asunto).[164] El plan preparado por el Equipo Themis nunca se llevó a cabo, tal vez como resultado de la propia filtración. Dicho plan se basaba en tácticas ilegales y sólo podía llevarse a la práctica en caso de que existiera una intención evidente de no proteger de la reacción violenta a las partes implicadas.

Más allá de cualquier posible perturbación directa, el contenido de los correos electrónicos de la empresa proporcionó gran cantidad de ideas a Anonymous y a otros interesados en las prácticas de seguridad empresariales. El espionaje y el sabotaje empresariales a trabajadores, organizaciones sin ánimo de lucro y activistas no son nada nuevo. Henry Ford confiaba en una unidad de seguridad interna al mando de Harry Bennett para intimidar a los trabajadores que intentasen sindicalizarse. Una empresa de seguridad privada llamada Pinkerton, fundada en 1850 y que aún hoy presta esos servicios, se hizo famosa por infiltrarse en los sindicatos y espiar a los trabajadores para sus clientes empresariales. De hecho, esta práctica es tan común que se le ha dado un nombre: "espionaje laboral". En épocas más recientes, Walmart ha sido duramente criticada después que se acusara a la empresa de ejercer una amplia vigilancia de «accionistas, críticos, proveedores, comité de dirección y empleados».[165]

En la actualidad, la industria de la vigilancia privada es un sector más sólido, rentable y amplio que nunca y presume de mantener estrechos vínculos con las agencias gubernamentales de tres letras (de hecho, muchos contratistas emplean a operativos entrenados por el gobierno y los militares). Un informe publicado en 2013 y titulado *Spooky Business* ("Un negocio espeluznante"), escrito por el Center for Corporate Policy, una organización sin ánimo de lucro cuyo objetivo es verificar el abuso empresarial, enumera más de una docena de ejemplos de espionaje e infiltración corporativos —muchos de ellos a base de tácticas estandarizadas estilo COINTELPRO— dirigidos contra grupos antibelicistas, ecologistas, que abogan por la seguridad alimentaria o

defienden los derechos de los animales y el control de armas, entre otros. Por tomar un ejemplo, el grupo ecologista Greenpeace ha sido sometido a numerosas infiltraciones ilegales; Électricité de France, por ejemplo, contrató a una empresa para hackear a Greenpeace Francia en 2006 y fue multada con 1,5 millones de euros cuando la acción fue descubierta.[166]

El informe transmite el inquietante problema actual de las infiltraciones en el mundo corporativo de la siguiente manera: «La capacidad de las empresas para el espionaje se ha disparado en los últimos años... Estos antiguos y actuales empleados del gobierno, y actuales contratistas del gobierno, llevan a cabo sus actividades de espionaje contra organizaciones sin ánimo de lucro *con escasa regulación o supervisión* y aparentemente con total impunidad.»[167]

Los servicios especializados de HBGary, que ofrecían "sofisticadas" operaciones de espionaje, no eran más que un pequeño jugador en una enorme industria. Sin embargo, un equipo de periodistas de Ars Technica, expertos en tecnología, después de hacer una cuidadosa selección de los correos electrónicos conseguidos por Anonymous y de redactar una docena de concienzudos informes (reunidos posteriormente en un libro) llegó finalmente a la conclusión de que «la capacidad de ataque del plan "La amenaza de Wikileaks" no era una simple bravuconería». HBGary era una empresa que estaba a la vanguardia de este tipo de servicios y había desarrollado un eficaz software antimalware y troyanos, rootkits y softwares espía personalizados que facilitaban un acceso no autorizado a los sistemas informáticos. HBGary también había ocultado un puñado de exploits de día cero —esas vulnerabilidades que no han sido reveladas públicamente— para su futuro uso, asegurando así un acceso directo a un número incalculable de redes, ordenadores y correos electrónicos. Según los documentos filtrados, HBGary proporcionó una memoria oculta de estos días cero, con el nombre en código Juicy Fruit, a una subdivisión de un contratista de Northrop Grumman llamada Xetron.[168]

La información pública acerca de este mercado de días cero fue prácticamente inexistente hasta que una serie de informes de investigación presentados entre 2012 y 2014 reveló que se trataba de una industria floreciente. Según *The New York Times*, estos exploits se pueden vender por precios que oscilan entre 35.000 y 160.000 dólares cada uno. Los gobiernos son los clientes que mejor pagan, asegurándose de esta manera un

significativo control de las vulnerabilidades. El gobierno de Estados Unidos, en particular, está considerado como un destacado cliente.[169] Los exploits pueden utilizarse con carácter defensivo, pero cada vez resulta más evidente que a menudo son «convertidos en armas y desplegados agresivamente para cualquier propósito, desde el espionaje gubernamental y corporativo hasta el fraude indiscriminado», como ha señalado el periodista especializado en tecnología Ryan Gallagher.[170]

Aunque la información pública disponible acerca de estas prácticas está aumentando lentamente, nuestra comprensión del fenómeno es aún incompleta y fragmentada. Esta labor la realizan o negocian principalmente empresas con mandatos más laxos y menos obligaciones de divulgación que sus homólogos del gobierno. Los correos electrónicos de HBGary y HBGary Federal ayudaron a llenar los vacíos, aportando un recordatorio de «cuánto de este trabajo se lleva a cabo de forma privada y al margen del control de las agencias del gobierno», según la conclusión de Nate Anderson.[171]

Es importante destacar que aquellos que revelaron esta información, a diferencia de la Comisión de Ciudadanos que destapó las acciones de COINTELPRO, no estaban buscando nada en particular. La naturaleza azarosa de estos descubrimientos contemporáneos no es privativa de Anonymous. Según *Spooky Business*, gran parte de lo que hoy sabemos sobre el espionaje corporativo «ha sido descubierto por accidente, derivado de brillantes golpes de suerte».[172] No obstante, podríamos sugerir que no se trató en absoluto de una cuestión de suerte, sino de un bienvenido bien público aportado por la curiosidad insaciable e ilimitada del hackeo, aunque impulsada por circunstancias externas. Los correos electrónicos de HBGary, por ejemplo, se obtuvieron gracias a la labor de hackers empeñados en la pura y simple venganza.

«Si podemos acceder a ese nivel de información, entonces somos una auténtica CIA privada –LOL»

Una semana antes de que su empresa fuese objeto de demoledores ataques, el fundador y director general de HBGary, Greg Hoglund, elogió a su equipo en una serie de correos electrónicos. Después de dar algunas

instrucciones relacionadas con la vigilancia de un creador de malware, Hoglund concluye el mensaje con una muestra de fanfarronería:

> Equipo,
>
> Buen trabajo. Comprobad este sitio http://www.freelancesecurity.com/ y encontrad a algún investigador que pueda llevar a cabo tareas de vigilancia y conseguir una identificación positiva de esta persona. He hablado con Penny y dijo que podría estar dispuesta a apoyaros contratando soldados en tierra enemiga para vigilar al objetivo. Espero fotos, lugar de trabajo, casa, quizás algunos socios. El sitio que he mencionado es solo uno, hay algunos más. Si podemos acceder a ese nivel de información, entonces somos una auténtica CIA privada LOL.[173]

Aunque Hoglund concebía su empresa como un sustituto más agudo, agresivo y modesto que los organismos de inteligencia encargados de hacer cumplir la ley, en la práctica HBGary se dedicaba fundamentalmente al negocio de desarrollar software antimalware y rootkits, herramientas furtivas de software que permiten al usuario acceder a un sistema informático sin ser detectado. Pero Aaron Barr, director general de la empresa subsidiaria HBGary Federal, que había sido creada por HBGary para conseguir lucrativos contratos del gobierno, quería expandir los servicios al terreno de la recogida de información. Esta intención quedó patente en el título de una charla programada para mediados de febrero de ٢٠١١ (pero cancelada debido a los hechos en cuestión) en una concurrida conferencia sobre seguridad que se tenía que celebrar en San Francisco: “¿Quién necesita a la ANS cuando existen las redes sociales?”

Barr obtuvo los datos para su presentación “infiltrándose” en Anonymous. ¿Su método? Durante gran parte de enero, utilizando el handle CogAnon, visitó los canales de IRC de AnonOps y la actividad correlacionada entre los canales de IRC y las redes sociales. En el IRC buscaba a alguien que colgara un enlace y luego se conectaba a Twitter para ver si el mismo enlace o tema aparecía al mismo tiempo, antes de deducir que el alias en el IRC y el perfil de Twitter estaban adjuntados a la misma persona. A finales de mes se había hecho con una lista de apodos, nombres

reales, cuentas de Twitter y ubicaciones de individuos que afirmaba que eran los principales jugadores de Anonymous. Según los correos electrónicos filtrados, el propósito de Barr era exponer a los operadores clave, ofrecer sus nombres al FBI y obtener un beneficio de estas revelaciones:

> De: Aaron Barr
>
> Tema: Enfoque de la presentación
>
> A: Mark Trynor, Ted Vera
>
> Fecha: Mié, 19 En 2011 12:14:26 -0500
>
> Vale, pues, el mes próximo daré una charla sobre redes sociales @ BSIDES SF. Creo que me centraré en sacar del armario a los principales jugadores del grupo Anonymous. Después de todo —¿nada de secretos, verdad? :) Veremos hasta dónde puedo llegar. Puedo centrarme un poco en la ANS solo para darles algo a todos esos chiflados de la libertad de expresión. Acabo de llamar chiflados a la gente que defiende la libertad de expresión, me he pasado un poco. Tíos, me encuentro en una posición extraña.

En otro correo electrónico le insiste a un colega programador —que ha cuestionado repetidamente la fiabilidad de las conclusiones de Barr— que «la venderé», refiriéndose a su lista de identidades.[174] (Finalmente, el codificador estaba tan preocupado por Barr que escribió un correo electrónico el 5 de febrero con una advertencia que resultaría premonitoria: «Creo que su arrogancia ha podido con él otra vez y eso es algo que nunca ha acabado bien... para ninguno de nosotros»).

Barr, por otra parte, pensaba que su operación iba viento en popa. ¿Cómo se enteró Anonymous de la infiltración de Barr en primer lugar? Aunque parezca increíble, Barr les sirvió la información en bandeja de plata al hacer público su proyecto. El departamento de relaciones públicas de HBGary le ofreció a Joseph Menn, periodista del *Financial Times*, una información sobre la próxima charla de Barr. Según me explicó Menn, él «respetaba el trabajo de la empresa afiliada a HBGary», y «puesto que la

estructura y rastreabilidad de Anonymous era un tema de gran interés», decidió seguir adelante con la publicación inmediata de la información. El 4 de febrero de 2011, Anons se despertó con esta noticia: «Es muy probable que una investigación internacional sobre ciberactivistas que lanzaron ataques contra empresas hostiles a WikiLeaks conduzca ahora al arresto de importantes miembros del grupo, después de que estos dejaran pistas sobre sus verdaderas identidades en Facebook y en otras comunicaciones electrónicas, según se afirma.» El artículo también incluía apodos y especulaciones sobre el lugar de residencia de estos participantes, unos datos que resultaron ser erróneos:

> Un importante miembro estadounidense de Anonymous, que utiliza el apodo en la red de Owen y con evidente residencia en Nueva York, parece ser uno de los individuos señalados en el curso de recientes investigaciones judiciales, según unas comunicaciones en línea reveladas por un investigador de seguridad privado... El Sr. Barr manifestó que Q y otras importantes figuras vivían en California y que la jerarquía era bastante clara, con otros miembros de primer nivel en el Reino Unido, Alemania, los Países Bajos, Italia y Australia.[175]

Si bien Owen y q (minúsculas) eran figuras prominentes, Owen vivía en Toledo, Ohio, y q residía, para ser más precisos, en el continente europeo.

Un artículo de fondo en una publicación respetada es un bien muy preciado. Si HBGary Federal era realmente una empresa tan formidable como para identificar a los tíos que movían los hilos detrás de Anonymous —antes incluso de que lo hiciera el FBI—, los ejecutivos corporativos, con buenas razones, estarían desesperados por contratarles. Las finanzas de la empresa estaban en la cuerda floja; un lucrativo contrato con el bufete de abogados Hunton & Williams cambiaría su suerte.[176] En una serie de comunicaciones internas, HBGary alardeaba sobre la pasta aparentemente garantizada:

> De: Aaron Barr
>
> A: Karen Burke, Greg Hoglund, Penny Leavy, Ted Vera

Tema: La historia realmente está tomando forma

Fecha: 05-02-2011

http://www.ft.com/cms/s/0/87dc140e-3099-11e0-9de3-

00144feabdc0.html

De: Greg Hoglund

A: Aaron Barr

Cc: Karen Burke, Penny Leavy, Ted Vera

Subject: Re: La historia realmente está tomando forma

Deberíamos postear esto en la página principal, enviar algunos tuits.

"HBGary Federal pone un nuevo listón como agencia de inteligencia privada", la broma sobre el listón es un lol deliberado.

—G

Estaban consiguiendo toda la atención que querían y, al principio, aparentemente solo de la buena. El FBI se puso en contacto con HBGary Federal el mismo día que se publicó la historia, solicitando una reunión para el lunes siguiente a las 11 de la mañana. Pero tal como lo expresó de manera memorable el humorista Stephen Colbert: «Anonymous es un nido de avispas y Barr ha dicho que meterá el pene dentro.»

Después de leer el artículo publicado en el *Financial Times*, los hackers que acababan de completar el ejercicio conjunto de "conquistar" los gobiernos de Oriente Medio estaban preparados para hacer ruido. El artículo contenía nombres de pila de muchos Anons y, después de la reciente tromba de arrestos de Anonymous en el Reino Unido y de las órdenes de detención en los Estados Unidos, la cuestión se consideró urgente. Sabu fue el primero en sugerir un ataque, motivado en parte por su profunda y arraigada hostilidad hacia los hackers de sombrero blanco y

hacia una industria de seguridad a la que consideraba un atajo de estafadores: software de seguridad de pésima calidad. Al principio algunos, pero no todos, estaban con él. Tflow recordó más tarde:

> <tflow>: al principio no apoyé esta idea, pensé que era una pérdida de tiempo y que alimentaría a los trols
> <tflow>: pero unos minutos más tarde Sabu encontró una vulnerabilidad sqli [interfaz de lenguaje de consulta estructurado] en el sitio hbgaryfederal.com
> <biella>: y el resto es historia
> <tflow>: sí

Con una vulnerabilidad demasiado buena como para ignorarla, todo el equipo se subió a bordo, accediendo a los sistemas de HBGary pisándole los talones al artículo publicado por el *Financial Times*. El equipo descargó montones de correos electrónicos de HBGary y HBGary Federal, borró un número incalculable de archivos y sus copias y, según se afirma, borró también los datos del iPhone y el iPad de Barr. Uno de los primeros correos electrónicos que encontraron incluía un PDF con los datos no filtrados que Barr había reunido sobre Anonymous. Muy pronto se dieron cuenta de que contenía innumerables errores. Muchos de los individuos de esa lista no habían hecho nada ilegal. Tal vez el problema evidente era el desconocimiento de Barr respecto de los operadores clave que estaban detrás de este hackeo: tflow, Topiary, Avunit, Kayla y Sabu. No era necesaria una infiltración profunda para determinar la existencia de muchos de estos participantes, como Topiary y tflow— miembros prominentes públicamente conocidos que pasaban mucho tiempo en canales de IRC abiertos, principalmente #reporter y #lounge.

Los hackers, aplicando un software de escaneo de seguridad diseñado para detectar vulnerabilidades conocidas, exploraron el sitio web de HBGary y encontraron rápidamente una vulnerabilidad en el CMS (sistema de gestión de contenidos) personalizado. Peter Bright, un periodista de Ars Technica que llevó a cabo una exhaustiva explicación de los detalles técnicos relativos a esta operación de hackeo, escribió que «de hecho, [el sistema de HBGary] tenía lo que solamente se puede describir como un bonito y enorme error de software en su interior».[177] Una vez dentro, los hackers hurgaron y encontraron contraseñas encriptadas. La encriptación era demasiado sólida para descifrarla solos, pero empleando la fuerza bruta

de un conjunto de GPU (unidades de procesamiento gráfico) pudieron descifrar los hashes (funciones de resumen) en pocas horas.

Una de las contraseñas, “kibafo33”, permitía el acceso a la cuenta de correo electrónico de Barr alojada en Gmail. Una vez allí, los Anons pudieron ver el exultante intercambio de correos internos de HBGary. Naturalmente, los hackers probaron la contraseña en todas las cuentas de Barr en las redes sociales y descubrieron que violaba la primera norma de seguridad de la información, que consiste en no utilizar nunca la misma contraseña en todas las plataformas. Ahora el equipo podía requisar todas las cuentas de Barr en las redes sociales para el lulz y cosas peores. Entrar fue solo el principio.

«El buen teatro debe ser drástico» 178

Era el domingo 6 de febrero de 2011, el día que se disputaba la Super Bowl. Millones de estadounidenses estaban pegados a sus televisores mirando cómo unos tíos enormes se molían a golpes con el propósito de conseguir meter un balón entre dos postes. Aaron Barr podría muy bien haber sido uno de esos espectadores, pero cualquier plan en ese sentido quedó eclipsado: había sido víctima de un hackeo brutal. Su cuenta de Twitter, pirateada, emitía las declaraciones más abyectamente racistas y degradantes posibles en 140 caracteres, junto con su número de la seguridad social y la dirección de su domicilio. Circulaban además innumerables imágenes de Barr poco favorecedoras y retocadas con Photoshop. Sus correos electrónicos, incluidos mensajes personales repletos de embarazosos detalles sobre sus problemas matrimoniales, fueron colgados en Pirate Bay.

En medio de todo esto, se conectó al servidor de IRC de AnonOps y fue invitado a participar en #ophbgary, un canal exclusivo. Barr aceptó la invitación:

> CogAnon (~CogAnon@an-33E99D21.dc.dc.cox.net) se ha unido a #ophbgary
> <q>: Hola CogAnon
> <tflow>: Hola, Sr. Barr.
> <Topiary>: El Sr. Barr y su infiltración en Anonymous; “Ahora nos están amenazando directamente”, ¿estoy en lo cierto?
> <tflow>: Pido disculpas por lo que está a punto de pasarle a usted y a su empresa.

<q>: ¿Disfrutando de la Superbowl, espero?
<CogAnon>: máximo un segundo. por favor
<tflow>: De verdad, Sr. Barr.
<tflow>: No tiene ni idea de lo que viene a continuación.
<Topiary>: tflow, ¿Cómo están las cosas en ese sentido, de todos modos?
<Topiary>: CogAnon es claramente súper 1337 con sus MP de habilidades en operaciones psicológicas en el área de Washington
<CogAnon>: De acuerdo... me imaginé que algo así podía pasar.
<Topiary>: CogAnon, no, no le gustará nada lo que viene a continuación
<tflow>: CogAnon, ¿puede adivinar lo que viene a continuación?
<Topiary>: ¡Ooh, un juego divertido - supongo!
<CogAnon>: tío... no lo entiendes. Era una investigación sobre las vulnerabilidades en las redes sociales... Nunca iba a publicar los nombres...
<Sabu>: MENTIROSO

Esta breve visita el domingo 6 de febrero fue el preámbulo de una conversación épica que tendría lugar más tarde ese mismo día. El chat que siguió a esa conversación se ha convertido en uno de los registros de acceso al IRC más vistos de la historia. El IRC representa una zona de libertad y autonomía en una Internet dominada por los intereses privados. Cuando se reúne a docenas, en ocasiones a centenares, de personas y se les da licencia para decir lo que les apetezca como quienesquiera que afirmen ser, es natural que aparezcan el humor, el ingenio, el dramatismo y, en ocasiones, el caos. Si el mundo es un escenario —y todos los geeks, hackers y hackeos cutres de InfoSec son meros actores— entonces, ¿en qué convierte eso a Internet? ¿En una obra dentro de otra obra, escrita en tiempo real, con cada actor colaborando línea a línea? Tienen sus entradas y salidas del escenario pero nada se conoce de antemano. El producto incluso parece un guión. La diferencia reside en que es popular, participativo e improvisado, acorde con las implicaciones y los desafíos del mundo real.

Primer acto

La obra que estábamos a punto de ver debe su existencia en parte a Barrett Brown. El domingo a última hora de la tarde trajo buenas noticias en #ophbgary, un canal cuyo propósito era debatir y celebrar el hackeo:

Laurelai>: BarrettBrown, ¿estás aquí?
<BarrettBrown>: Estoy en el teléfono con la presidenta de HBGary
<Sneux>: lol

Sabu lanzó la siguiente sugerencia:

<Sabu>: BarrettBrown, dile a PENNY que venga aquí y hable.

En este punto ya era de público conocimiento que Anonymous había participado en un festival de hackeo contra HBGary Federal y HBGary. La sugerencia de Sabu parecía una burla, no una petición real. Después de todo lo que había pasado, no parecía verosímil que Penny Leavy, la presidenta de HBGary, se arrojara al epicentro del nido de ratas que en ese momento estaban dedicadas a destrozar su empresa. Pero eso fue exactamente lo que hizo. Sabu inició el intercambio recordándole los incómodos hechos:

<Sabu>: penny. antes de comenzar— sepa que todos hemos visto las comunicaciones por correo electrónico entre usted y todo el mudo en hbgary. de modo que mi primera pregunta sería ¿por qué permitió que aaron vendiera semejante basura bajo el nombre de su empresa?
<ComradeBush>: jesús cristo [en español en el original]
<Sabu>: Penny, ¿sabía usted también que aaron estaba vendiendo información no fiable/equivocada/falsa que puede llevar al posible arresto de personas inocentes [?]

Ella sale en defensa de Aaron Barr:

<Penny>: Sabía que él estaba haciendo una investigación sobre las redes sociales y el problema asociado a ellas, la facilidad de fingir ser uno de vosotros
<Penny>: Nunca estuvo en sus planes entregar la investigación al gobierno. Nunca iba a publicar nombres, solo hablar de los handles
<Sabu>: Penny, si lo que está diciendo es verdad, ¿por qué entonces Aaron se reunirá mañana a las 11 con el FBI? POR FAVOR RECUERDE QUE TENEMOS TODOS SUS CORREOS ELECTRÓNICOS.
<Sabu>: muy bien penny como ya he dicho 4 veces tenemos todos los correos electrónicos. Hay montones de correos en los que usted fomenta la investigación de aaron... de modo que siento curiosidad
<heyguise>: aún estoy ordenando los correos
<Penny>: Creo que lo que él estaba haciendo era bueno, era informativo y arrojaba luz sobre un montón de cuestiones asociadas a las redes sociales

Los correos electrónicos filtrados contenían incontables pruebas de que Barr estaba dispuesto a reunirse con las autoridades y a sacar un beneficio de ese encuentro. Anonymous elaboró un plan financiero propio en IRC sobre la marcha, una propuesta de chantaje a la manera de Robin Hood:

> <Sabu>: penny. no apuntaremos a hbgary.com. está hecho. lo que puede hacer ahora es desviar sus inversiones de hbgaryfederal al fondo para la defensa de bradley manning y distanciarse de la investigación de aaron barnetts
> <Agamemnon>: Penny ... estamos siendo atacados de maneras que usted no entiende. No solo son los federales... los luchadores de la ‘libertad’ de la derecha tratan de quitarnos de en medio... los infiltrados nos han hecho daño... la investigación de Aaron contiene información personal de gente que nunca hizo nada más que asomarse por aquí... por favor trate de entender nuestra ira

Mientras tanto, el teléfono sonó en casa de Brown. En el otro extremo de la línea estaba nada menos que Barr. Ambos mantuvieron una educada conversación que se prolongó durante once minutos (Brown grabó la conversación y luego la subió a la red). Había cierta incertidumbre con respecto a qué pensaba hacer exactamente HBGary con esos datos. Barr, cuya voz no mostraba ningún signo de amargura, temor o siquiera enojo, se presentó con confianza: «Soy un contratista federal que trabaja principalmente en el ámbito de la seguridad.» Previendo una pregunta sobre sus motivos, Barr afirmó, «nunca he tenido intención de vender los datos al FBI». Los correos electrónicos mostraban claramente que se había puesto en contacto con el FBI y estaba buscando obtener un beneficio económico mediante la recopilación de estos nombres correlacionados y “descubriendo” a Anons, según sus palabras. Presumiblemente un montón de organizaciones sitiadas estarían interesadas en averiguar la identidad de sus asaltantes. Independientemente del resultado final, las revelaciones desprendidas de los correos electrónicos fueron recibidas como una inquietante amenaza por el conjunto de la comunidad de Anonymous.

Barr le ofreció a Brown unos motivos muy diferentes, afirmando que su programa general era demostrar los puntos débiles de las redes sociales y exponer la jerarquía que se esconde detrás de la colmena. «Claramente hay una estructura», dijo. Brown asintió hasta cierto punto —«Estoy de acuerdo en que unas docenas de personas son las que marcan el paso»— pero señaló que muchos de los nombres no eran correctos. «Nunca pretendí que fuese

exacto al 100 por cien», insistió Barr, incluso en su conversación con el *Financial Times*. «El periodista escribe lo que quiere escribir.» Barr le recordó a Brown que aún tenía intención de reunirse con el FBI a la mañana siguiente, señalando que [el asunto] «no estará en mis manos».

Los correos electrónicos filtrados indican que, de hecho, Barr y sus colegas habían dedicado una gran atención —solo ese día— a la cuestión de entregar los nombres al FBI. Ted Vera, presidente y director de operaciones de HBGary Federal, cerró el tema en favor de no hacerlo:

> Podrías acabar acusando a una persona equivocada. O podrías enfurecer aún más al grupo. O podrías estar equivocado y que te explote en la cara, y en la cara de HBGary, públicamente. La insinuación de que tienes sus verdaderos nombres es suficiente. No hay necesidad de hacerlos públicos. Mañana te reunirás con el FBI. Dudo de que ellos compartan mucha información pero pueden, de manera informal o inadvertida, examinar algunos de tus hallazgos.

Anonymous, por su parte, publicó el documento pero también divulgó cómo se había equivocado Barr con la mayoría de los nombres.

Al igual que había hecho con Leavy, Brown intentó atraer a Barr para que participara por la red. «Les gustaría que viniese. Intentaré mantener las cosas productivas», le dijo Brown. Barr, que ya se había conectado temprano ese mismo día, se resistía; entonces Brown, con su acento tejano, cambió de estrategia. «Entiendo que haya tenido un día difícil —dijo Brown—. Ha sido acosado. Repito, no tuve participación en eso, aunque no puedo decir que lo desaprobara porque estamos aquí para protegernos a nosotros y a nuestros intereses.» Hacia el final de la conversación telefónica, no quedó claro si a Barr le habían convencido para que volviera a disputar un segundo asalto.

Una vez terminada la conversación telefónica y nuevamente en el IRC, Brown, un apasionado de los vídeojuegos, declaró que ya se había cansado de «esta estupidez» y anunció su intención de «jugar un rato a *Fallout: New Vegas*». Pero antes, cuando Anonymous le hizo una serie de preguntas, Brown manifestó un característico gesto de empatía hacia Leavy:

> <Penny>: Gracias a todos fue muy agradable hablar con vosotros. ¿Como puedo

volver a conectarme con vosotros?
<Sabu>: penny, ¿puede hacer que greg se acerque a su ordenador y hable con nosotros unos minutos /?
<BarrettBrown>: Si hace que se sienta mejor, soy adicto a los opiáceos y aún estoy en tratamiento con suboxona
<BarrettBrown>: que acabaré en un par de días
<Penny>: Eh Sabu gracias por ser tan amable, un día duro
<Sabu>: está todo bien. Un día duro también para nosotros

Segundo acto

Mientras Penny abandona el escenario, Greg Hoglund hace su entrada, reemplazándola físicamente ante el ordenador:

Penny es ahora conocida como greg
<evilworks>: éxito
<q>: éxito épico
<greg>: Lo siento tíos era yo era mi ordenador y greg se ha largado
greg>: ha regresado
<Sabu>: ok
<Sabu>: ¿GREG ES USTED?
<greg>: sí

Antes de que Anons reanudara su interrogatorio, hicieron una pausa para un momento de autofelicitación:

<`k>: Greg ¿ha oído hablar alguna vez de las claves ssh? [las claves ssh se refieren a la tecnología de encriptado]
<Sabu>: ante todo, si aún no lo ha leído eche un vistazo en http:// pastie.org/1535735
<Sabu>: fue así cómo nos hicimos con rootkit.com
<evilworks>: oh wow Sabu
<q>: esa es buena
<q>: :)
<q>: qué empresa de seguridad que tenéis
<Sabu>: ¿hay alguna cosa que pueda hacer para impedir que utilice el nombre de su empresa // hbgary?

Se produjo una llamativa pausa mientras Greg miraba el sitio copiado y

pegado, donde se detallaba un registro de la filtración. Captó de inmediato la extrema gravedad de la situación:

<greg>: de modo que entonces también tenéis mi cola de correos electrónicos
<Sabu>: sí greg.
<`k>: greg lo tenemos todo
<Agamemnon>: Greg, siento curiosidad por saber si entiende lo que pretendemos hacer ¿Entiende por qué hacemos lo que hacemos?

«Lo tenemos todo.» Si esta obra se hubiera escenificado, es probable que en este punto Hoglund se hubiera embarcado en un soliloquio lamentándose por su suerte o, como mínimo, hubiera transmitido cierto grado de horror facial. Hoglund debió comprender que sus opciones eran ciertamente limitadas. Pero si no eres capaz de embaucar a los embaucadores, siempre se puede apelar a la razón... ¿tal vez?

<greg>: ¿os dais cuenta de que si publicáis mi cola de correos electrónicos eso provocará daños de millones de dólares a HBGary?
<c0s>: greg, creo realmente que la gente aquí es muy sincera cuando dice que estaría encantada no publicando los correos electrónicos. Pero su decisión estará basada en lo que suceda con Aaron.
<c0s>: que es la razón por la que le pregunté si es posible que nos explique sus ideas sobre lo que se podría hacer aquí.
<c0s>: para que ellos pudieran tener una idea de lo que usted puede hacer.
<Sabu>: greg, en esencia lo que queremos es que usted y su empresa se distancien de aaron
<BarrettBrown>: Como he dicho, es un momento perfecto para hacer una donación a Túnez
<evilworks>: o a Bradley Manning
<evilworks>: cualquiera de los dos

¿Daría resultado su sincera exhortación? Con la reaparición de otro personaje principal pasamos al acto final de la obra.

TERCER ACTO

CogAnon entra en la sala.
<Sabu>: es aaron

<Sabu>: coganon
<Sabu>: es su APODO DE ESPÍA
<Sabu>: hola aaron
<c0s>: Buenas tardes Aaron.

Hoglund se tomó un momento para desvincularse de Barr:

<greg>: aaron es director general de su propia compañía, que lamentablemente comparte el nombre de HBGary – no puedo hacer otra cosa que gritarle por teléfono
<`k>: jajaja están todos aquí
<greg>: hbgary (mi hbgary) tiene el 15% de la propiedad de hbgary federal, para que conste
<greg>: sí, y aaron tenía que pinchar el nido de avispas verdad
<evilworks>: estoy descargando algunos correos electrónicos

Gracias a los correos electrónicos sabemos que las alegaciones de Hoglund en este caso son en gran parte palabras huecas. Barr era un miembro importante y respetado del equipo de gestión de HBGary:

De: Greg Hoglund

A: all@hbgary.com

Tema: ¡Bienvenidos Aaron Barr y Ted Vera al equipo de gestión de HBGary!

Date: 23-11- 2009

¡Estoy entusiasmado de anunciarles que Aaron Barr y Ted Vera se han incorporado al equipo de HBGary! Ted y Aaron gestionarán y dirigirán HBGary Federal, una empresa subsidiaria de HBGary, centrada en la contratación en el ámbito gubernamental. Ambos cuentan con una vasta experiencia y recientemente han desarrollado un negocio de 10 millones de dólares anuales en Northrop Grumman. Ambos han ganado y dirigido proyectos de desarrollo multimillonarios y gestionado equipos muy importantes. Conocemos a Aaron y Ted desde hace más de 5 años. Son dos jugadores de primera categoría en el espacio de contratación DoD y son capaces de “recorrer los pasillos”

en los espacios de los clientes. La semana pasada, operadores muy importantes les hicieron ofertas a Ted y Aaron, y ellos eligieron a HBGary. Esta actitud se refleja perfectamente en nuestra empresa. Los jugadores de primera atraen a jugadores de primera. Aaron ocupará el cargo de Director General de HBGary Federal y operará fuera del área del DC. Ted asumirá el cargo de Presidente y Director de Operaciones de HBGary Federal y su área de operaciones estará en Colorado Springs. ¡Bienvenidos a bordo!

—Greg Hoglund

Director General, HBGary, Inc.

Hoglund cambió entonces el enfoque, apelando al supuesto sentido de autoconservación de Anonymus:

<greg>: tíos, ¿os dais cuenta de que atacar a una empresa estadounidense y robar datos privados es algo que nunca habéis hecho antes?
<greg>: no, creo que tendríais que haber tenido en cuenta vuestra reputación pública –no tiene buena pinta.
<Agamemnon>: Greg. Conteste por favor: ¿entiende quiénes somos y por qué hacemos lo que hacemos?
<CogAnon>: Yo nunca iba a vender, se han equivocado.
<evilworks>: no nos IMPORTA nuestra reputación
<Sabu>: greg, nuestra reputación no está en juego. La suya sí.
<greg>: quiero decir, esto fue un hackeo en toda regla, y por cierto tengo que reconocer que realmente nos habéis hackeado bien
<evilworks>: hacemos lo que creemos que es correcto
<c0s>: Greg, y a la gente aquí no le importa en absoluto la reputación
<evilworks>: hay muchas maneras de hacernos quedar mal
<evilworks>: no nos importa
[...]
<Baas>: De acuerdo, vosotros no le pasáis exactamente información a las autoridades... Pero es la idea lo que cuenta. Queremos que la reputación de Aaron quede destrozada por esto.
<evilworks>: jesús

Brown, tomándose un descanso de su videojuego, envió un recordatorio:

< BarrettBrown>: se reunirá con el FBI mañana a las 11, no lo olvidéis
<c0s>: Eso es lo que más me molesta.
<Sabu>: eligió gente al azar en facebook y los relacionó con apodos en el irc
<BarrettBrown>: y sin duda me expondrá personalmente

Mientras la ira aumentaba a su alrededor, Barr seguía sin dar su brazo a torcer:

<evilworks>: ¿por qué empezó a trabajar en esto en cualquier caso?
<BarrettBrown>: Como le dije a él, los federales jodieron a mi familia
<evilworks>: ¿fue por interés personal, por una investigación?
<CogAnon>: ¿queréis que responda?
<CogAnon>: tíos, de todos modos no importa... habéis publicado mis correos electrónicos.
<evilworks>: sospecho que es por un beneficio económico
<Sabu>: greg. conteste por favor
<CogAnon>: lo hice por la investigación.
<CogAnon>: El fbi me llamó debido a mi investigación.
<CogAnon>: el correo electrónico al que os referís sobre la venta de datos se trataba de un modelo creado a partir de esta clase de investigación.
<c0s>: o bien lo sabía, o es usted un completo idiota, usted SABÍA que sus métodos eran deficientes.
<CogAnon>: Los máximos datos que pensaba mostrar era un organigrama de IRC con iconos que representaban aquellos apodos que pensé que conocía...
<evilworks>: todavía quedan algunos correos electrónicos que no hemos publicado
<Sabu>: aaron, tiene que disculparse con nosotros, con sus inversores en hbgary y dejar las cosas claras
<Sabu>: que usted NO identificó a la dirección de anonymous
<Sneux>: ^
<Sabu>: y que su investigación es puramente académica y teórica

Con todo lo dicho hasta ese momento, Barr había tenido bastante:

<CogAnon>: muy bien chicos tengo que irme a la cama. Repito que esto era solo una investigación sobre las vulnerabilidades de las redes sociales... os habéis pasado de la raya...
<c0s>: esto fue ojo por ojo por parte de gente a la que usted perjudicó.
<Sabu>: lo hizo doxeando a gente jodidamente inocente
<Sabu>: que le den de verdad
<evilworks>: ¿Que le den y ya está?

<Sabu>: mira los nombes en tu documento
<Agamemnon>: joder
<Baas>: El problema es que ni siquiera consideró que había hecho algo mal.
<Sabu>: no tiene problemas en doxear a gente inocente
<Sabu>: QUIERO DECIR LA GRAN PUTA
<Agamemnon>: Greg, haga un trato ahora... ciérrele la boca... todo irá bien
<greg>: ¿trato? ¿qué clase de trato?
<Agamemnon>: Aaron cierra la puta boca... tus correos electrónicos siguen siendo privados
<owen>: tíos
<owen>: controlaros
<CogAnon>: era solo una investigación.

Uno de los beneficios de mirar una obra por Internet es que nadie sabe qué pasará a continuación y que puedes hablar todo lo que te apetezca sin molestar a nadie. Hasta ahora era más que sabido que yo era la antropóloga residente. Un Anon me envió un mensaje privado para pedirme que reflexionara sobre ese momento:

<PKE>: bien, ¿cómo te sientes observando todo esto?
<biella>: hola PKE
<PKE>: ¿disfrutando de la vista?
<biella>: en gran parte
<biella>: estoy un poco enferma en este momento de modo que estoy luchando con todas las vistas
<PKE>: como outsider, ¿cuál es tu opinión hasta ahora?
<biella>: ¿de anonymous?
<PKE>: bueno, eso es muy general
<PKE>: me refería al implacable desmantelamiento de hbgary and co

Me resultaba un poco difícil mantener la conversación. Estaba en medio de una horrible gripe y me preocupaba que fuese el presagio de una rabia completa. Me habían administrado la última inyección hacía cuatro días, después de un desafortunado encuentro con un murciélago el mes anterior. A través de la bruma, la fiebre y la garganta irritada, le dije:

<biella>: me sorprendió la rapidez con la que sucedió todo
<biella>: al principio
<biella>: y luego la conversación en el canal ha respondido bastante al espíritu del

lulz
<biella>: que tal vez estuvo sumergido durante semanas en las otras operaciones

A lo que PKE, a salvo tanto de la gripe como de mis postulados irracionales sobre la aparición de la rabia, contestó con un comentario más incisivo:

<PKE>: totalmente
<PKE>: quiero decir
<PKE>: se hizo un gran trabajo
<PKE>: pero hubo un gran déficit de lulz
<biella>: sí y ahora ha sido repuesto
<PKE>: creo que esto es algo más que un superávit
<biella>: jaja es verdad
<PKE>: no se me ocurre una operación de anonymous más ridícula en la historia reciente
<biella>: la conversación en el canal ha sido irreal
<biella>: los mensajes de tweter fueron indignantes
<biella>: sí
<biella>: es verdad
<PKE>: colega. Nunca había entendido realmente el atractivo de la máquina del odio de internet antes de esto
<PKE>: Dios mío, cuando mezclas a sociópatas con altruistas cabreados, mejor te apartas del puto camino

Al final, insatisfechos con lo que los simples mortales tenían que ofrecer, los embaucadores de Anonymous optaron por hacer públicos los correos electrónicos adicionales de HBGary que se habían estado reservando como un as en la manga. Mientras que la mayoría de los correos electrónicos de la empresa era seleccionada para su publicación durante la conversación por chat, a la semana siguiente Anonymous también publicó 27.606 correos electrónicos de Greg Hoglund en AnonLeaks.[179]

UN EQUIPO DE NINJAS DE ANONYMOUS DESENMASCARA AL EQUIPO THEMIS

Durante los días posteriores a este épico enfrentamiento, el lulz palpitó a través de los canales de chat del IRC, electrificando y recargando el ánimo

colectivo. La prensa no pudo obtener el hilo del hackeo. Los periodistas se lanzaron a la búsqueda de Barrett Brown para que hiciera algún comentario, que finalmente apareció desde la NPR (Radio Pública Nacional) hasta la BBC. El 8 de febrero de 2011, Brown declaró exultante en #ophbgary:

<BarrettBrown>: La NPR me preguntó quién hizo lo de HBGary
<BarrettBrown>: Les dije "un equipo de ninjas de Anonymous".
<FEAR_Anonymous>: ¿La NPR?
<DingDong>: JAJA
<DingDong>: ¡sí!
<FEAR_Anonymous>: LOL
<HateIRC>: lol guays
<Sci>: lmfao [parténdome el puto culo de la risa

Desde fuera, daba la impresión de que Brown era un amado activista de Anonymous en su máximo esplendor. Pero desde dentro, husmeando solo un poco, era fácil asistir a las quejas sobre el papel que Brown había asumido de un modo demasiado voluntario. En aquel momento, en Anonymous eran aficionados a elaborar colectivamente los documentos escritos. La mayoría de ellos se referían a las operaciones que se llevaban a cabo. Un poco después, aquel mismo mes, apareció un documento con el título "Todo sobre Barrett Brown. Añada sus comentarios". Esta revisión de desempeño de facto diseccionaba sus aportaciones —consiguiendo asistencia jurídica, redactando editoriales, captando a la prensa en línea— en relación con una evaluación moral de su comportamiento público. Nada de esto se hizo a sus espaldas. De hecho, antes de que se publicasen las críticas recibidas le pidieron que escribiera una declaración, incluida aquí en su totalidad, para que apareciera cerca del inicio del documento:

> Sí. Cualquiera que no sepa lo que he hecho para Anon no ha participado en OpTúnez y OpEgipto en ninguna medida real, y cualquiera que no haya trabajado en esa campaña cada puto día puede irse a tomar por culo. Lo que es jodido es cuánta más gente está en este documento que en cualquiera de los documentos realmente importantes de Anons. Ésta es la "declaración", queridos. Solo añadir que la persona que comenzó todo esto no consiguió que su párrafo se incluyera en el comunicado de prensa y está molesto por eso. —Barrett

Brown

Comprensiblemente —teniendo en cuenta que él acababa de mandar a todo el mundo a tomar por culo— la mayoría de las siete páginas restantes de comentarios describiendo su personalidad, motivos y contribuciones tendían a lo negativo. Las críticas, aunque salpicadas con ocasionales valoraciones positivas, encontraron consenso en cuanto a la oposición a su autobombo:

> —Esto es importante. Es sobre los principios básicos de la ideología de Anonymous, el anonimato y la igualdad de todos.
>
> —Pareces dar a entender que eres tan especial e importante que los principios mencionados más arriba, anonimato e igualdad de todos, no se aplican en tu caso.
>
> * Tu dedicación no está en discusión. Eres casi con toda seguridad uno de los amigos más importantes de Anons. Solo quiero decir que no quiero verte como ‘líder de Anonymous’ ni como su portavoz. Sé que eso no sería beneficioso para Anonymous.+1 sinceramente +1 indudablemente +1
>
> * @Barrett: Anonymous te apoyará siempre que no formes un ejército personal y te abstengas de líderfagging. +1+1+1

El pequeño equipo de hackers que trabajaba entre bastidores también estaba muy lejos de sentirse satisfecho con toda la atención mediática que Brown estaba recibiendo a raíz de la operación HBGary. Aproximadamente un mes después, Adrian Chen y John Cook, de Gawker, publicaron un artículo, “Dentro de la sala de guerra secreta de Anonymous”, detallando las consecuencia del hackeo de HBGary. Brown había hablado largo y tendido con los periodistas:

> Barrett Brown, generalmente considerado por los miembros de Anonymous como portavoz del grupo, dijo que conocía el “fallo de seguridad” desde hacía algún tiempo: «Éramos conscientes del fallo de seguridad ya que otros registros de ‘HQ’ habían sido posteados antes

> (y de todos modos debo señalar que HQ no es realmente HQ —advertiréis que la verdadera coordinación de los hackeos realizados no aparecerán en esos registros)».[180]

Después de leer el artículo, muchos de los hackers, ya molestos con Brown, se enfurecieron y comenzaron a atacarle en #anonleaks, el canal dedicado a debatir las filtraciones de HBGary.

> <tflow>: es irónico que declares que eres bueno jugando con los medios de comunicación cuando no lograste que entendieran correctamente los hechos básicos

Brown, junto con Gregg Housh (c0s), que también hablaba frecuentemente con los medios de comunicación, culparon a los periodistas de identificar a un portavoz cuando se les había dicho que no lo hicieran.

> <c0s>: Hoy me han llamado dos personas y al final de las entrevistas ambas me preguntaron
> <c0s>: “podemos llamar a su portavoz”
> <BarrettBrown>: escuchad a Housh
> <c0s>: tuve que hacer un gran esfuerzo cada vez para conseguir que esos idiotas no lo hicieran
> <c0s>: y algunos accedieron a no hacerlo
> <c0s>: y lo entiendo totalmente
> <c0s>: ellos lo ponen correctamente y luego tienen editores que lo “arreglan”
> <c0s>: y ponen portavoz o alguna otra estupidez
> <BarrettBrown>: eso mismo
> <BarrettBrown>: discutid con Housh
> <c0s>: es una puta mierda tratar con estos gilipollas
> <c0s>: no
> <c0s>: yo no discuto eh
> <tflow>: entonces ve y que los maricones de los editores lo arreglen

Con esa cuestión solucionada pasaron a otros temas molestos, principalmente cómo Brown había afirmado tener conocimiento interno de #HQ, el fallo de seguridad de HBGary, y de la operación de hackeo, cuando él no había presenciado la operación y mucho menos contribuido a ella. Peor aún, simplemente estaba equivocado sobre #HQ; había sido allí donde se había coordinado el hackeo a HBGary:

<`k>: pss [para ser sincero], no hay necesidad de que siquiera hables con los medios de comunicación en primer lugar aún no has hecho nada y sin embargo tienes una explicación para todo
<BarrettBrown>: k, he hecho algunas cosas, querido
<tflow>: también me jode cómo le haces declaraciones a gawker sobre #hq
<FriedSquid>: sugerencia: ser periodista consiste, en cierta medida, en que tu mensaje llegue, exponer tu trabajo. Hacer que tu nombre sea conocido.
<BarrettBrown>: ¿podemos dejar de hablar de esto?
<tflow>: cuando no te concierna a ti en lo más mínimo
<BarrettBrown>: ellos me hicieron las putas preguntas
[...]
<tflow>: entonces no abras la boca y diles que no te concierne si no te concierne
<BarrettBrown>: no, que te jodan oh dios mío
<`k>: es fácil decir que “no” a los periodistas
<BarrettBrown>: yo no obedezco órdenes
<tflow>: si no sabes de lo que estás hablando

Como había sido el caso con Snapple antes que el suyo, Brown fue desterrado momentáneamente del canal, en este caso por `k. A ello siguieron comentarios finales, incluyendo algunos sobre la calidad del espectáculo, como si las discusiones se hubieran duplicado en una versión improvisada de una competición de debates en el instituto:

<Earnest>: odio tomar partido pero`k y tflow hicieron un trabajo mucho mejor que barret en esta ocasión
<tflow>: le hubiese echado a patadas
<tflow>: pero no me gusta echar a patadas a la gente
<tflow>: de los chats
<`k>: me enferman estos maricones que buscan la atención en los medios de comunicación cuando dicen que no han participado en las cosas y sin embargo creen que lo saben todo

En el momento en el que Brown era asediado debido a sus actividades promocionales en relación con los hackeos, la propia HBGary se enfrentaba a otra serie de desafíos difíciles y decisiones necesarias.

Las consecuencias

Un día después de chatear con Anonymous y una semana antes de que se anunciara la fecha prevista para la inauguración de la conferencia de seguridad más importante de Estados Unidos, organizada por RSA Security Inc., Greg Hoglund se lamentó de su situación ante un periodista: «Me están causando un gran dolor en este momento... Lo que están haciendo ahora no es hacktivismo, es terrorismo. Aquí han cruzado realmente una línea roja.»[181] La acusación de terrorismo era nueva, nunca había aparecido, ya sea públicamente o en correos electrónicos de Hoglund o Barr. La inversión de los términos era probablemente una táctica cuidadosamente diseñada por el departamento de comunicación para describir a estos hackers como "terroristas" y, de este modo, como un grave peligro para la sociedad; era quizás una declaración calculada para convertir la embarazosa realidad del espantoso hackeo —un (probable) desastre potencial— en una ventaja. Hoglund también tomó la decisión de anular la conferencia de la RSA.

Aunque HBGary había elegido claramente un camino complicado, la empresa salió ilesa de esta crisis, o tal vez incluso reforzada, ayudada por su nueva calificación de Anonymous como elemento "terrorista" del que había sido víctima. Un año más tarde, HBGary fue adquirida por una empresa contratista de defensa llamada ManTech International. Hoglund cooperó estrechamente con las autoridades en sus investigaciones sobre Anonymous, como quedó debidamente reflejado en un comunicado de prensa del FBI:

> El amplio caso instruido contra seis hackers, incluido [Héctor Xavier] Monsegur, [alias "Sabu"], es el producto de una vasta investigación... El ataque contra HBGary fue cuidadosamente investigado por el FBI en Sacramento y el caso se transfirió a Nueva York a petición de Monsegur. Cabe señalar como dato importante que la investigación realizada en Sacramento se benefició en gran medida de la ayuda de la propia HBGary.[182]

A Aaron Barr y HBGary Federal la jugada no les salió tan bien. Como director general, a Barr no podían despedirle, pero decidió abandonar la empresa a finales de febrero de 2011 y, posteriormente, la empresa cerró sus puertas. Durante una entrevista con Parmy Olson, de la revista *Forbes*, Barr

reflexionó sobre lo que había ocurrido: «¿Si me arrepiento [de haber hecho esas declaraciones] ahora? Por supuesto... estoy recibiendo amenazas personales y tengo dos hijos. Tengo dos hijos de cuatro años. No hay nada que valga eso.»[183]

Los otros dos miembros del Equipo Themis, Berico y Palantir, que habían conspirado con HBGary Federal para desacreditar a WikiLeaks, se lavaron sus ensangrentadas manos como Lady Macbeth, cortando de inmediato todos los lazos con HBGary Federal y negando tener ningún conocimiento del mencionado plan. Pero tal como explicó Nate Anderson de Ars Technica, «ambas direcciones del Equipo Themis en estas empresas sabían exactamente lo que se estaba proponiendo (es posible que ese conocimiento no haya llegado a las altas esferas). Vieron los correos electrónicos de Barr y utilizaron su trabajo. Sus ideas acerca de atacar a WikiLeaks hicieron que Palantin se inclinara casi literalmente hacia las 'tácticas proactivas'.»[184]

Después, preocupados por su reciente conocimiento de semejantes tácticas, un grupo de miembros demócratas del Congreso pidió investigar al Equipo Themis. En el curso de una entrevista, el presidente del comité, Hank Johnson, explicó por qué apoyaba esa investigación: los dólares del contribuyente estadounidense se estaban utilizando para financiar herramientas y programas concebidos para espiar a los ciudadanos y reprimir los derechos que proclama la Primera Enmienda.[185] Otros congresistas, principalmente el representante Lamar Smith, desmantelaron y bloquearon discretamente esta investigación. Lamentablemente, los principales medios de comunicación nunca siguieron de cerca este asunto para escribir sobre la desaparición de la investigación.

La creciente insatisfacción con Barrett Brown dentro de Anonymous no le hizo reprimirse. Brown permaneció activo dentro de Anonymous durante algunos meses más. El portal íntimo en una empresa de seguridad privada como HBGary Federal impulsó a más voluntarios a contribuir a un *think tank* basado en la web, el Proyecto PM (PPM), «una wiki de colaboración abierta centrada en los contratistas de inteligencia del gobierno» que Brown había creado en 2010. Para él resultaba evidente que HBGary Federal no era precisamente una anomalía entre los contratistas de defensa. En un artículo de opinión publicado en 2013, Brown expresó sus objetivos para PPM: «no debemos fijarnos solamente en las agencias de tres

letras (FBI, ANS, CIA) que nos han traicionado sistemáticamente en el pasado, sino también en el número indeterminado de contratistas de inteligencia privados que han surgido en los últimos tiempos para traicionarnos de una manera más eficiente y orientada al mercado.»[186]

El enorme tamaño de esta industria mercantilista ha sido cuidadosamente evaluado por Tim Shorrock, uno de los pocos periodistas de investigación que ha investigado exhaustivamente el tema. La información es escasa, según explica, pero hay algunos detalles reveladores que sugieren la magnitud de estas operaciones:

> La externalización se ha vuelto tan generalizada que, el año pasado, el Director de Inteligencia Nacional decidió estudiar el fenómeno. Pero cuando finalmente se completó el informe en abril de 2007, los resultados fueron aparentemente tan asombrosos que el DNI vetó la idea de dar a conocer el informe y, en cambio, les comunicó a los periodistas que la revelación de las cifras sería perjudicial para la seguridad nacional.[187]

Se calcula a partir de las cifras actuales disponibles que el 70 por ciento de los 80.000 millones de dólares del presupuesto de Estados Unidos destinado a inteligencia se canaliza hacia contratistas privados.[188] Si bien los correos electrónicos de HBGary y HBGary Federal no aportaron cifras concretas sobre la dimensión de la industria en su conjunto, sí ofrecían medidas cualitativas que apuntan a la escala masiva del mundo de la contratación de inteligencia del gobierno. Brown, con la colaboración de voluntarios que le ayudaron a llevar a cabo la investigación y redactar el artículo (y se encargaron de todo el trabajo técnico), presentó un depósito central para catalogar el mejor de los mundos de las corporaciones que se especializan en recogida de información, espionaje e infiltración para clientes corporativos y gubernamentales. Donde los documentos filtrados realmente surtieron efecto fue en aportar detalles sobre el tipo de tácticas empleado por las empresas privadas en la era de las tecnologías digitales y en red. Las empresas, evidentemente, estaban dispuestas a proponer y a participar en actos temerarios. Después de todo, Barr estaba en camino de proporcionar datos de inteligencia fiables, por ejemplo, doxeando a algunos Anons que no habían hecho nada ilegal, facilitando incluso apodos y ubicaciones a un

periodista. Su empresa también había diseñado planes detallados para sabotear la carrera de un periodista. Puesto que esta clase de trabajo se halla ahora repartida entre cientos de empresas privadas diferentes, es poco probable que exista alguna vez una única publicación masiva de documentos equivalente a la que rompió COINTELPRO detallando el rostro corporativo del espionaje. En cambio, la opinión pública tendrá que confiar en los datos en batería fragmentados que recibe a través de filtraciones y hackeos como el de HBGary.

Inspirados por el éxito del hackeo contra HBGary, otros Anons buscarían muy pronto dirigir técnicas similares hacia otras empresas de seguridad e inteligencia. Pero primero, los hackers que habían diezmado HBGary Federal se separarían de AnonOps para embarcarse en un viaje de cincuenta días como compañía experimental de performances bajo el nombre de LulzSec. El grupo recibió críticas muy favorables de los internautas. Pero las corporaciones contemplaban la obra, con su aparentemente interminable cadena de bises, completamente horrorizadas.

Capítulo 8

LulzSec

LulzSec —un equipo de hackers renegados de Anonymous que rompió con el colectivo y se duplicaron como juglares itinerantes— apareció unos meses después del tristemente célebre hackeo a HBGary Federal. Integrado por los mismos individuos que habían hackeado a Aaron Barr con una intención claramente vengativa, la asombrosa carrera catalizadora de cincuenta y cinco días emprendida por LulzSec se inició a comienzos de mayo de 2011 y acabó abruptamente el 25 de junio, poco después de que uno de los suyos, Sabu, fuese detenido y convertido en menos de veinticuatro horas por el FBI. Entre sus objetivos se encontraban Sony Music Entertainment Japan, Sony Pictures Entertainment, Sony BMG (Holanda y Bélgica), PBS, el Departamento de Protección Civil de Arizona, el Senado de Estados Unidos, el Organismo de Lucha contra la Delincuencia Organizada Grave del Reino Unido, Bethesda Softworks, AOL y AT&T. A pesar de esta actividad frenética —y numerosas intrusiones— cuando se lo compara con Anonymous, LulzSec era un grupo más manejable y contenido, al menos desde una perspectiva organizativa. Sus miembros hackeaban con absoluta impunidad, haciendo finalmente buena la afirmación hecha en 2007 en Fox News de que Anonymous estaba compuesto por tíos “chutados de esteroides”.

Los miembros de LulzSec desempeñaban su papel totalmente conscientes de actuar para un público variopinto. Incluso los más arrogantes hackers de seguridad que antes habían desdeñado a Anonymous animaban ahora a LulzSec. Algunos sombreros negros de la vieja escuela vivían indirectamente a través de LulzSec, superados por su soberbia, su actitud de jódete-todo-está-permitido y su insaciable apetito por poner en evidencia el

patético estado de la seguridad en Internet. Los periodistas no podían conseguir información suficiente de sus bufonadas y tampoco eran realmente capaces de mantenerse al día. Con un número tan exagerado de intrusiones, exfiltraciones y volcados de datos, LulzSec hizo estallar en pedazos el habitual ciclo de noticias de tres días. Durante buena parte de su reinado, LulzSec tentó a los periodistas con el señuelo de la información para luego someterles al tratamiento del silencio, con una única y notable excepción: Parmy Olson, de la revista *Forbes*. Estos hackers le suministraban (casi) exclusivamente información sobre sus actividades y, para conservar sus privilegios, ella guardaba discreción acerca del acuerdo que tenían.[189]

Aunque a Parmy Olson le proporcionaban suficiente información para que pudiera escribir sus artículos, las principales salidas de LulzSec al mundo exterior eran su sitio web, su cuenta de Twitter y el sitio web Pastebin.com, donde se reflejaban todas sus descargas de datos y se publicaban sus proclamas. Pastebin es utilizado habitualmente por los programadores para colgar pequeños fragmentos de texto, códigos fuente o información sobre configuración. El sitio genera una URL especial que luego puede ser pegada en otra parte, como el IRC, para que otros lo vean. En lugar de pegar un texto multilineal en canales de IRC —una acción que te valdría la expulsión de un canal por “inundarlo”—, se puede simplemente facilitar el enlace. Normalmente, estos enlaces generados son caracteres triviales aleatorios y se pueden programar para que expiren al cabo de un tiempo. Pastebin es solo uno entre una multitud de sitios de esas características, de modo que el motivo que impulsó a LulzSec a elegir este medio es un tanto misterioso. En cualquier caso, libró a LulzSec de la necesidad de disponer de una infraestructura para sus misivas. Su cuenta de Twitter acumulaba multitud de seguidores, en ocasiones hasta veinte mil por semana. Redactadas por su embaucador residente, las actualizaciones deliciosamente elaboradas de Topiary exhibían a menudo un aire marítimo.

El equipo de LulzSec navegaba por alta mar, aventurándose en aguas internacionales con la bandera pirata ondeando en lo alto del mástil, montando un espectáculo para que los demás lo disfrutaran. Durante una entrevista que le hice a David Mirza, un sombrero negro retirado, observó:

LulzSec impactó en Internet con una actitud de sombrero negro mucho

> más potente —y reconocible de inmediato como auténtica— que la estructura de Anonymous de la que habían surgido. Acertaron con la arrogancia y el estilo. Admitían cosas, mostraban documentos, impartían justicia. Nadie podía atraparlos y ellos lo sabían. Su campaña se convirtió en una saga genial que hizo que algunos que ya habían vivido esa aventura volvieran a sentirse como adolescentes.

Con un tuit, la revista y organización de los hackers *2600: The Hacker Quarterly* (una publicación especializada en información técnica) reflejó el sentimiento general de la comunidad: «Sitios web hackeados, infiltración/escándalo corporativo, guerras en el IRC, nuevos grupos de hackers obteniendo titulares en todo el mundo… ¡los noventa han vuelto!»[190]

Ningún pirata que se respete puede zarpar sin un navío y la tripulación de LulzSec se alineaba detrás del timón de un barco bautizado *Louise*. El nombre derivaba de la interpretación errónea de un periodista —y de la defectuosa pronunciación resultante— de la palabra LulzSec. Y puesto que sus dependencias eran infinitamente espaciosas, decidieron llevar a bordo una mascota. El clásico loro de los piratas fue sustituido por una colorida bestia felina: un afable gato gris llamado *Nyan Cat*, conocido entre los internautas frecuentes porque iluminaba hasta el cielo más oscuro emitiendo permanentemente por el culo un chorro de arco iris. Este divertido disparate era atenuado por el portavoz y logotipo virtuales de LulzSec: un monigote con bigote de villano, bien afeitado y de estilo francés, además de monóculo, chistera y traje de tres piezas, y bebiendo, naturalmente, una copa de buen vino. Este refinado caballero apareció por primera vez en un *rage comic* en español (un meme-comic popular entre los geeks de Internet) antes de que LulzSec lo adoptara en marzo de 2011. Los admiradores hablaban del personaje sin nombre «como si fuese un señor»; hasta que se le acabó conociendo simplemente como “el señor”. Todo esto no hizo más que imbuir a LulzSec de una mezcla quimérica de profundidad, mística y mitología memética nunca vista hasta entonces en los grupos de hackers de Anonymous. Un Anon que también había desarrollado actividad en la escena de los sombreros negros, me lo describió de esta manera en una entrevista: «LulzSec parecía tener una especie de mito completamente formado ya de entrada, mientras que a otros grupos de hackers como Cult

of the Dead Cow les llevó décadas conseguir eso.»

Volviendo a la realidad por un momento —más tarde exploraremos las cuestiones relativas a la fantasía— debemos señalar que estos hackers se congregaban en su propio canal privado de IRC, donde estaban protegidos del drama que por entonces devoraba a AnonOps. Liberados del imperativo categórico de la moralfaggotry, ellos también podían hackear a quienes les apeteciera y por cualquier razón que se les antojara.

Quizás resulte sorprendente oír que LulzSec surgió, completamente formado, de una única conversación corriente en el IRC. Resulta menos sorprendente cuando uno descubre que estos hackers estaban un poco aburridos con Anonymous y —algunos de ellos, al menos— se habían cansado de trabajar en las operaciones de otros. Los embaucadores ociosos son capaces de cualquier cosa con tal de acabar con el aburrimiento. También ayudó el hecho de que tuviesen un cache de datos robados de Fox News esperando a ser descargado y que AnonOps estuviera sumido, en ese momento, en un caos creciente.

El infierno no tiene tanta furia como los videojugadores despreciados

Durante la mayor parte de marzo y abril de 2011, AnonOps no había reducido en absoluto su actividad desde donde los habíamos dejado la última vez, pero la red estaba plagada de una creciente letanía de problemas. Empezaron a surgir pequeños incendios y el desgaste de apagarlos comenzó a hacer mella en el grupo.

Aunque la crucifixión de Aaron Barr a manos de Anonymous le convirtió en el hazmerreír de Internet de 2011, la misión de buscar y revelar las identidades legales de Anons no desapareció con él. Backtrace Security (su nombre es una referencia jocosa a una conocida trolescapada de Anonymous realizada en 2010 contra una preadolescente, Jessi Slaughter, cuyo padre afirmó haber “rastreado” –*backtrace*– a Anonymous) convirtió este objetivo en su misión principal y recogió el testigo donde lo había dejado Barr. El miembro más crítico de la organización, Jennifer Emick, había sido guerrera de Anonymous en otro tiempo, durante la lucha emprendida con el Proyecto Chanology contra la Iglesia de la Cienciología,

pero se volvió crítica con las más que cuestionables tácticas empleadas luego por AnonOps (las mismas que LulzSec aprovecharía más tarde como su más valioso juego de herramientas). Emick, autoproclamada defensora de la ley y el orden, declaró que «uno no puede luchar por la justicia y la democracia con tácticas injustas y antidemocráticas».[191] Era un buen argumento, pero omitía la ética cuestionable de su propia marca de vigilancia, puesto que a mediados de marzo de 2011 Backtrace había publicado un organigrama con las "identidades" de setenta participantes y afiliados de Anonymous. Como ya ocurrió en la intentona de Barr, muchos de esos nombres eran erróneos o ya eran públicos. Todos excepto uno. El mérito hay que concedérselo a Backtrace; se trataba del nombre individual más importante en aquel momento: Héctor Xavier Monsegur, el famoso hacker Sabu. (El documento de Backtrace incluía un pequeño error en el apellido de Sabu, Montsegur.)

Backtrace no doxeó a Sabu gracias a una proeza de reconocimiento inteligente; simplemente tuvieron un golpe de suerte cuando una participante de Anonymous, que respondía al nombre de *Laurelai* y había pasado algún tiempo en los canales más reservados, entregó tontamente a Emick sus registros de chat. El bloque de texto —más de doscientas páginas de archivos de registros— incluía una pista que conducía directamente a una sala de estar nuyorriqueña* en el Lower East Side de Manhattan. Mientras chateaba con sus compatriotas, Sabu había tecleado o pegado accidentalmente una dirección de web que incluía el dominio de su servidor personal: prvt.org. Una vez que Backtrace introdujo esta dirección de web en Google descubrieron uno de sus subdominios, que incluía a su vez otros datos personales que, inevitablemente, les llevaron a su página en Facebook.

El documento de Backtrace, llamado "Namshub" (palabra sumeria que significa "conjuro"), fue diseccionado en trozos por Anonymous, pero la mayoría de la gente, por supuesto, no pudo menos que evaluar de un modo realista la veracidad de su propia salida del armario. Sabu —y tal vez un puñado de sus colegas y hackers más íntimos de antaño— sabía que había quedado expuesto. Al doxearlo, Backtrace actuó como la fuerza de Eshu, el embaucador de las encrucijadas, dejando caer a la poderosa figura en el cruce de caminos. Sabu/Monsegur se encontraba ante una decisión trascendental. Después de haber visto su nombre en la pantalla podría haber

borrado todo el contenido del ordenador, desaparecido y regresado años más tarde como un héroe hacker. Es verdad que no hubiera podido desvanecerse de inmediato. Hacerlo habría significado confirmar que «le habían doxeado», tal como tflow se encargó de recordarme. Pero podría haberse marchado un mes después de que las acusaciones hubiesen perdido fuerza. Él ya era un hacker legendario y con su ausencia su protagonismo no habría hecho más que aumentar. En palabras de un Anon, Sabu era toda una leyenda. Si Monsegur hubiera optado por apartarse de la circulación durante algún tiempo para volver a aparecer después de que expirase el estatuto de limitaciones, podría haber regresado a su querida *Isla del encanto* (Puerto Rico), refugiado para entretener a sus amigos y familia con relatos sobre sus hazañas. Dejarlo habría sido la maniobra más inteligente, pero a Sabu lo perdía la arrogancia.

Por el contrario, buscó a Emick y la bombardeó con información falsa para sembrar la confusión; uno de sus colegas hackers explicó que «cuando Backtrace publicó su lista doxeada, intentó engañarles para que creyeran que en realidad era un agente doble que trabajaba para un ISP (proveedor de servicios de Internet) y que trataba de infiltrarse en Anonymus, pero ellos no se lo tragaron».

Aunque Sabu era muy conocido entre sus colegas, generalmente mantenía un perfil público discreto, hasta que fue doxeado por Backtrace. Poco después envió un tuit por primera vez:

> ¡Hola! Estos días actúo bajo el nombre de Sabu. He creado esta cuenta para aclarar algunas cosas, especialmente después de las filtraciones de #backtraceinsecurity.

Sabu continuó paseando por Trickster Lane (la senda de los embaucadores), incluso de una manera más pública que antes, convencido de ser intocable, hasta que un año más tarde se supo que era un informante. (Tras salir de prisión, Sabu renacería como el azote de Anonymous. El día de su puesta en libertad, un ex íntimo compatriota hacker declaró sin reservas en el IRC: «Es mejor pasarse quinientos años entre rejas que mirarse al espejo y saber que das asco.»)

Pregunté a unos cuantos hackers cómo respondieron a los intentos de doxeo como Namshub. Uno de los pocos hackers principales de LulzSec

que, por lo que sabemos, nunca fue identificado o atrapado me dio una razón dividida en cuatro partes, que coincidía con los sentimientos que había visto expresados por otros hackers:

<Avunit>: A) Confías en que los demás [se] protegen lo suficiente de modo que no tiene importancia
<Avunit>: B) Todo va bien y quieres mantenerte unido a los demás porque funciona
<Avunit>: C) No te preocupan los nombres
<Avunit>: D) De todos modos, el nombre podría estar equivocado, ¿no?

El 1 de abril de 2012, poco después del envenenado doxeo Namshub de Backtrace, AnonOps lanzó la Operación Sony. «Preparaos para el mayor ataque jamás visto, al estilo Anonymous», declararon en un vídeo.[192] AnonOps comenzó a saturar la PlayStation Network de Sony con una campaña de DDoS, interrumpiendo el servicio y a los videojugadores que lo utilizaban. Para entender por qué AnonOps lanzó este ataque debemos retroceder a enero de 2011, cuando Sony demandó a un precoz y escandaloso hacker estadounidense llamado George Hotz, más conocido por su handle, “geohot”. Su especialidad en el mundo del hackeo es el llamado *jailbreaking*, que consiste en liberar dispositivos destinados a los consumidores, como los iPhones y las consolas de videojuegos, del control de la empresa propietaria para modificarlos como le apetezca a su usuario. Habitualmente, esta operación implica un análisis inteligente del dispositivo, la redacción de un software que desactiva los controles de copia y acceso y la liberación de documentación para todo el proceso, de modo que otros puedan hacer lo mismo. Este tipo de hackeo recicla los dispositivos de función única al estado preferible de un ordenador de función general. Aunque un dispositivo de función única es útil para personas que no quieren saber nada de aparatos complicados, muchos técnicos consideran esta restricción una limitación arbitraria de su derecho fundamental a utilizar su propiedad como quieran. Ellos también consideran el jailbreaking un desafío atractivo, como si la empresa hubiera creado un puzzle especial para que ellos lo resolvieran.

Hotz se ganó los elogios de hackers y de algunos defensores de los derechos digitales en 2007 como el primer hacker que, con diecisiete años, desbloqueó al operador del iPhone. Luego, a finales de 2009, colocó en su

agenda técnica la popular PlayStation (PS3) de Sony. Hotz y un equipo anónimo llamado “fail0verflow” (no asociado a Anonymous) consiguió romper el bloqueo en solo cinco semanas. El 26 de enero de 2011 repartió su amor colgando instrucciones de jailbreaking para la PS3 en su sitio web, lo que atrajo muchísima atención. El jailbreaking de la PS3 permite que el usuario de la consola de videojuegos lleve a cabo una serie de funciones que no podrían hacerse en una PS3 normal: jugar a juegos pirateados, crear copias de seguridad, jugar directamente desde el disco duro (acelerando notablemente el tiempo de carga), reproducir vídeos, instalar GNU/Linux y, tal vez lo más importante, crear, innovar y aprender de maneras muy diversas. Cuando la BBC le entrevistó sobre esta proeza, Hotz parafraseó un dicho clásico entre los hackers: «se supone que [La PS3] es *inhackeable*, pero *nada es inhackeable*.»

Las grandes empresas, naturalmente, tienen también sus propios dichos, uno de los cuales podría formularse de esta manera: «Tú hackeas, nosotros denunciamos.» Poco después de que Hotz publicase las instrucciones relativas al jailbreaking, Sony le demandó por infracción de copyright y violación de la Ley de Abuso y Fraude Informático. Conocido por decir siempre lo que piensa, al oír la noticia Hotz no se quedó cómodamente sentado, sino que habló en voz muy alta. Bueno, técnicamente estaba sentado y, más que hablar, rapeó (y desde que fue publicada en YouTube, su respuesta fue vista más de dos millones de veces). Sentado en una silla y vestido con una vieja camiseta azul, en su anodina habitación, empezaba diciendo: «Ey, soy geohot y, para quienes no lo sepan, Sony me ha demandado.» Golpea su cuerpo al son del ritmo, sus infantiles rizos marrones se agitan mientras describe a Sony como “envasadores de chapuzas” y acaba con un: «Pero joder tío / ellos son una corporación / y yo soy una personificación / de la libertad para todos.»[193]

La demanda civil de Sony no solo mencionaba a Hotz y a otros numerosos hackers, sino también a un centenar de “Fulanos de Tal”, algunos de los cuales se sospechaba eran miembros del equipo de hackers anónimo de Hotz. Sony acusó incluso a aquellas personas que simplemente habían visto las instrucciones de Hotz sobre el jailbreaking. Un aviso legal a su proveedor de la web exigía las direcciones de IP de los visitantes al sitio de Hotz entre 2009 y 2011. Se solicitó a YouTube que entregase información sobre aquellas personas que habían visto el vídeo de Hotz

sobre jailbreaking o colgado comentarios sobre el mismo. Muchos geeks de Internet estaban conmocionados por la demanda presentada por Sony. Este sentimiento quedó bien reflejado por el autor de ciencia ficción y defensor de Internet Cory Doctorow, quien opinó que era «absurdo e injusto que una multinacional gigantesca utilizara sus enormes recursos legales para aplastar a un hacker solitario cuyo 'delito' es averiguar cómo pueden hacer cosas (legales) con algo de su propiedad.»[194]

Anonymous entró en la pelea. El hecho de que Hotz nunca buscase ayuda (de hecho, no quería tener nada que ver con Anonymous) es irrelevante. El primer anuncio de Anonymous decía:

> Estimados ~~hijoputas avariciosos~~ SONY,
>
> ¡Felicidades! Ahora tenéis la atención de Anonymous. Vuestras acciones legales recientes contra compañeros internautas, GeoHot y Graf_Chokolo, han sido consideradas como una ofensa imperdonable contra la libre expresión y la libertad en Internet, fuentes fundamentales del libre lulz (y sabéis muy bien lo que pensamos del lulz). Habéis abusado del sistema judicial en un intento de censurar información sobre cómo funcionan vuestros productos. Habéis victimizado a vuestros propios clientes simplemente por poseer y compartir información, y continuáis persiguiendo a aquellos que buscan información. Al hacerlo, habéis violado la privacidad de miles de personas inocentes que solo aspiraban a la libre distribución de información. Vuestra supresión de esta información está motivada por la avaricia empresarial y el deseo de ejercer un control absoluto sobre las acciones de los individuos que compran y usan vuestros productos, al menos cuando esas acciones amenazan con socavar el dominio corrupto que intentáis mantener sobre el copywrong, perdón, el "copyright".[195]

La operación declinó rápidamente. El ataque DDoS contra la Playstation Network de Sony (PSN) no contribuyó a que Anonymous ganara nuevos amigos, sino más bien la indignación de videojugadores que echaban chispas al verse privados de su fuente de entretenimiento. En medio del doseo se formó un grupo disidente autodenominado "SonyRecon" con el

objetivo de dosear a los ejecutivos de Sony. Esta jugada demostró ser controvertida entre los activistas de Anonymous y su amplia red de apoyo.

Espoleado por la inmediata impopularidad de la operación, Anonymous hizo pública la siguiente declaración: «Nos hemos dado cuenta de que apuntar al PSN no es una buena idea. Por lo tanto, hemos suspendido temporalmente nuestra acción hasta que encontremos un método que no perjudique gravemente a los clientes de Sony.» Esperaban que esto bastaría para apagar el incendio.

Durante todo el mes de abril, sin embargo, la PSN siguió teniendo problemas. Puesto que Anonymous había organizado inicialmente la operación, muchos asumieron de manera natural que la horda de activistas enmascarados era responsable de la persistencia de los problemas. Pero aunque se produjeron algunas reivindicaciones dispersas de responsabilidad, Anonymous finalmente y de manera inequívoca insistió, «Por una vez no hemos sido nosotros».

A falta de una declaración oficial por parte de Sony, los rumores y las insinuaciones continuaron creciendo. Después de semanas de silencio, el 26 de abril Sony publicó una declaración: «Hemos descubierto que, entre el 17 y el 19 de abril de 2011, cierta información del servicio de cuentas de usuario de la PlayStation Network y Qriocity se vio comprometida a causa de una intrusión ilegal y no autorizada en nuestra red.»[196] Millones de números de tarjetas de crédito se vieron afectados, provocando que Sony instara a sus clientes a que cambiaran sus contraseñas y permanecieran alerta ante cualquier indicio de fraude. Pero las cosas no hicieron más que empeorar con el anuncio de que la PSN permanecería inaccesible. Colin Milburn, un académico y ávido videojugador, escribió un relato fascinante sobre el terrible hackeo a la PSN desde la perspectiva de los videojugadores despreciados, como él mismo. En su texto apuntó: «Llegados a este punto, la marea emocional se convirtió en indignación, gran parte de la cual estaba dirigida a Sony por sus laxas medidas de seguridad, pero mucho más contra los hackers que habían perpetrado la intrusión.»[197] Finalmente, la inactividad de la PSN se prolongó durante veintitrés insoportables días.[198]

Hacia finales de mayo, Sony afirmaba que este hackeo les había causado unas pérdidas de 171 millones de dólares.[199] Aunque Sony nunca aportó datos sobre sus pérdidas económicas, estos hechos provocaron una debacle que le costó a la empresa dinero, tiempo y reputación. Los

ejecutivos de Sony, a los que finalmente se llamó a testificar ante el Congreso de los Estados Unidos, fueron amonestados por las reprobables prácticas de seguridad de su organización y los retrasos en notificar a los clientes. En el Reino Unido, Sony fue multada con 250.000 libras esterlinas por la Oficina del Comisionado de Información, que señaló claramente la responsabilidad de la propia empresa:

> Si son ustedes responsables de tantos detalles de tarjetas de pago y de tantos detalles de conexión, mantener seguros esos datos tiene que ser su prioridad. En este caso no fue así, y cuando la base de datos fue asaltada —si bien en un ataque criminal definido—, obviamente las medidas de seguridad implementadas no eran lo bastante buenas.[200]

En medio de esta crisis, los ejecutivos de Sony intentaron desviar la culpa hacia Anonymous, afirmando que habían encontrado un archivo dejado en el servidor del grupo que identificaba a Anonymous como parte responsable. Pero ningún hacker de Anonymous o LulzSec ha admitido nunca ni ha sido acusado de este delito (y cinco de ellos, junto con dos asociados, han sido declarados culpables de numerosos delitos de hackeo, lo que conllevó el decomiso de sus discos duros para practicarles un análisis forense). El hackeo de la PSN, un misterio en 2011, sigue sin resolverse.

«Blanqueando pasta, canalizando bitcoins, estafando con PPI, creando botnets, descargando bases de datos.»

El drama que rodeó la obstrucción provocada por OpSony en la PlayStation Network proporcionó el contexto inmediato para la gestación de LulzSec. A mediados de abril, un puñado de hackers en #internetfeds consiguió abrirse camino hacia fox.com y robar la base de datos de sus ventas. Junto con información personal sobre empleados y periodistas de Fox, el material robado incluía más de setenta mil direcciones de correo electrónico y contraseñas de personas que se habían registrado para recibir actualizaciones sobre las convocatorias de audiciones en el próximo concurso de talentos de la cadena, *El factor X*. Los datos permitieron asimismo que Anons requisaran unas cuantas cuentas de Twitter de Fox

News. Puesto que en los últimos tiempos Fox no había hecho nada censurable —aparte de seguir existiendo— estos hackers se sintieron en apuros. Dejar el doxeo y los datos corporativos bajo el control de Anonymous probablemente les acarrearía fuertes críticas por parte de las bases del colectivo, una conclusión que provocó que los Anons que habían obtenido la base de datos pensaran en alternativas. El miembro más joven del grupo, tflow, tenía una sugerencia a mano, inspirada ligeramente en Goatse Security, el equipo de seguridad/troleo de weev, que había publicado datos capaces de avergonzar a AT&T:

<tflow>: tendríamos que crear un competidor de Goatse Security
<tflow>: aquel hack por el lulz
<tflow>: Lulz4u Security
<pwnsauce>: LOL sí
<pwnsauce>: ¿tflow te has conectado desde anoche??
<tflow>: ¿adónde?
<pwnsauce>: Necesitamos recuperar shell
<pwnsauce>: uhm
<tflow>: pregunta a X
<pwnsauce>: creo que está utilizando su teléfono para esto

Para introducir el nombre “LulzSec”, tflow recurrió a un clásico intemporal de Internet, el arte ASCII (técnica de diseño gráfico que utiliza ordenadores para su presentación):

<tflow>: ( ) ( )( )( ) (_)/. |( )( ) / __)(___)/ __)
<tflow>:)(__)(__)( )(__ / /_(_ _))(__)(__ \ )__)((__
<tflow>: (____)(______)(____)(____) (_)(______) (___/(____)___)
<tflow>: “Lo hicimos por el lulz” ~LulzSec
<pwnsauce>: GUAI
<pwnsauce>: ¿hacemos una desfiguración de página?
<pwnsauce>: POR CIERTO, hoy estuve pensando
<Palladium>: jaja
<tflow>: LulzSec, división lulz de los InternetFeds
<Palladium>: estoy más a favor de los hackeos orientados políticamente
<tflow>: sí
<tflow>: pero
<tflow>: ¿qué podemos hacer con fox.com?
<tflow>: ¿excepto desfigurarla por el lulz?

<tflow>: no hay nada político en eso
<tflow>: no es como cuando desfiguramos pm.gov.tn
<pwnsauce>: lol

Por alguna razón, la propuesta de tflow no cuajó de inmediato. Le pregunté la razón y él no pudo recordarla. Tal vez no había suficiente gente conectada para alcanzar un consenso, o quizás quienes estaban conectados a un IRC estaban distraídos con otras tareas. Hay ocasiones en que las conversaciones en IRC resultan difíciles de explicar, incluso en el momento, y a toro pasado es mejor no dedicarles demasiado razonamiento lineal. De modo que ni siquiera voy a intentarlo, al menos en este caso. Lo que sí sabemos es que tflow abandonó temporalmente Anonymous después de pelearse con un operador temperamental que estaba a punto de activar la red de AnonOps. Y tflow no fue el único. Otros también se tomaron unas breves vacaciones, solo para regresar al 4 de mayo:

<Sabu>: tflow el guapo ha vuelto
<Falcon>: buen rollo
<tflow>: ¿qué hay de nuevo?
<Falcon>: muchas cosas tflow, es bueno verte otra vez
<pwnsauce>: YUPI
<Falcon>: soy Topiary por cierto
<Sabu>: ;p
<Sabu>: la buena noticia es que tflow ha vuelto

Reunidos y de buen rollo pero, ¿no habría sido mejor haber tenido una razón para descargar los datos de Fox? Ahora la debacle sufrida por Sony dejó doblemente claro que los hackeos aleatorios podían provocar la ira de Anonymous en general, de modo que había una presión aun mayor para no hacer públicos los datos en nombre del colectivo. Se plantearon publicarlos en 4chan, para «filtrarlos como anonymus en minúsculas», según me explicó tflow. Sabu lanzó la idea de entregarle los datos a la periodista de *Forbes* Parmy Olson, esperando que «tal vez le dé un empujoncito para escribir su libro». Como sabemos los escritores, no hay nada como una enorme cantidad de datos de contraseñas y correos electrónicos corporativos para ponerte en el estado de ánimo adecuado para un ataque de escritura. (Si me hubiesen entregado los datos a mí, este libro se habría

publicado al menos un año antes.) Pero ninguna de estas ideas estaba cuajando realmente. Al final Topiary, que durante el último mes se había mantenido en silencio en AnonOps pero seguía activo en los canales secretos, ingresó en el IRC bajo el nombre de Falcon. Mientras Sabu sugería filtrarle los datos a Olson, Topiary sugirió filtrarlos a través de la cuenta de Twitter de LulzLeaks:

<Falcon>: un momento, vamos a filtrarlos bajo @LulzLeaks
<Falcon>: nuestro twitter

tflow volvió a sacar otra vez el nombre LulzSec, esta vez con un poco más de énfasis, puesto que antes no había convencido:

<tflow>: debemos establecer una marca imo pseudo-lulzsec
<tflow>: me gusta
<Sabu>: también que alguien contacte con parmy
<tflow>: Lulz4u Security
<Sabu>: decidle que tenemos una nueva filtración para ella
<Sabu>: exclusiva
<tflow>: Goatse Security
<pwnsauce>: SÍ
<pwnsauce>: tflow—me gusta
<Falcon>: Parmy está durmiendo
<Sabu>: pues que levante el culo de la cama
<Sabu>: jajaja
<Sabu>: pensad en un nombre guai tíos
<Sabu>: rápido
<tflow>: ¿Lulz4u Security?

Sabu estaba impaciente:

<Sabu>: bueno
<Sabu>: por qué no hacemos esto simplemente bajo el banner de anonleaks
<Sabu>: ?
<tflow>: porque
[...]
<pwnsauce>: me gustan LulzLeaks y Lulz4u Security

Otros miembros objetaron, nuevamente, que se hiciera una distinción entre

filtración ética y no ética:

<tflow>: anonleaks es para filtraciones éticas
<lol>: :D
<tflow>: :P
<Falcon>: http://twitter.com/#!/LulzLeaks
<lol>: no :D
<lol>: ¿acaso importa?
<Falcon>: ¡LulzLeaks!
<lol>: no hackear y recuperar datos es ético xD
<pwnsauce>: tenemos el twitter LulzLeaks xD
<Falcon>: esto es lo que deberíamos hacer:
<Falcon>:—subir DB
<Falcon>:—recuperarlos en LulzLeaks
<Falcon>:—retuitear desde tuiters oficiales de Fox News

Después de proponer algunos otros nombres posibles, como “Ninjasec”, finalmente se pusieron de acuerdo en LulzSec. Con el nombre ya acordado comenzaron a analizar la publicación y las ilustraciones:

<Sabu>: Lulz Security / lulzsec
<Falcon>: quiero poner a Batman follándose a un tiburón como imagen
<Falcon>: pero ya la quemé
<Sabu>: lol
<Sabu>: bueno mantengamos esos nombres durante una semana o así
<Sabu>: hagamos que la filtración del factor x llame la atención
<Sabu>: luego maltrataremos a los gerentes/ventas de fox
<Sabu>: luego avergonzaremos al fbi con infragard
<Falcon>: alguien que consiga que @lulzsec aparezca en todas partes
<Falcon>: noticias, /b/, en alguna parte donde se difunda
<Falcon>: AnonOps

Cuando algo es nuevo y brillante tiene sentido presentar una introducción:

<tflow>: ¿redactamos una declaración?
<Falcon>: No estoy seguro de qué podríamos escribir... hmm.
<Falcon>: Supongo que podríamos presentarnos.
<Falcon>: Como LulzSec.

En tres minutos, Topiary creó una. Luego lo celebró con... galletitas:

<Falcon>: Hola, buenos días y ¿cómo estáis? ¡Fantástico! Somos LulzSec, un pequeño equipo de individuos lulzy que cree que la monotonía de la comunidad virtual es una carga para lo que realmente importa: la diversión. Considerando que ahora la diversión está limitada al viernes, donde todos esperamos ansiosamente el fin de semana, fin de semana, hemos asumido la responsabilidad de difundir alegría, alegría, alegría a través de todo el calendario. Como introducción, por favor ved...
<Falcon>: ...debajo la información de contacto de los concursantes de Factor-X 2011. Podéis esperar más cosas en el futuro y si sois como nosotros y os gusta ver cómo otra gente se vuelve loca, visitad nuestro twitter! twitter.com/LulsSec
<tflow>: perfecto
<Falcon>: aunque es @LulzSec
<Falcon>: joder tío lo escribí a bote pronto en 2 minutos, vuelvo en seguida, voy a buscar una galletita

Topiary y Sabu aportaron predicciones proféticas:

<Sabu>: oh tío lol
<Sabu>: será divertido
<Falcon>: LulzSec a tope
<Falcon>: blanqueando pasta, canalizando bitcoins, estafando con PPI, creando botnets, descargando bases de datos
<Falcon>: el lulz que hacen sigue adelante

Todo este bombo, sin embargo, cayó en saco roto. La primera descarga tuvo escaso impacto en los medios de comunicación. LulzSec era todavía un grupo completamente desconocido; después de todo era viernes, un día horrible para difundir algo en los medios de comunicación. Y así los hackers, seguros en su recién encontrada identidad como LulzSec, pudieron concentrarse en el jugoso chismorreo sobre un operador de AnonOps llamado Ryan Cleary, quien se acababa de convertir en un canalla.

Cleary, que dirigía una numerosa botnet, era uno de los operadores más poderosos e impopulares en la red de IRC de AnonOps. En numerosas ocasiones escuché quejas sobre su conducta errática, que se traducía en excluir aleatoriamente a los participantes en canales privados y públicos. Poco después de la creación de LulzSec, saltó la noticia de que Cleary había doseado la red de AnonOps que una vez había ayudado a administrar.

También reveló más de seiscientos nombres y direcciones de IP de usuarios de la red de IRC. (AnonOps practicaba la política de no conservar las direcciones de IP después de que alguien se desconectaba, pero durante la conexión AnonOps tenía acceso a las direcciones de IP de todos los usuarios que no estaban protegidos por una VPN [red privada virtual].) ¿Por qué lo hizo Cleary? Después de demasiados conflictos con otros operadores había decidido tomarse la revancha. Al mismo tiempo, según uno de sus colegas hackers, Cleary quería impresionar a un grupo hacker underground llamado Hack the Planet, más conocido simplemente como HTP. Desde 2011 hasta 2013, según un hacker que seguía al grupo, HTP se mostró sumamente activo y en posesión de «una extensa e impresionante lista de cosas». Desde entonces el grupo ha pasado a retiro pero HTP sentía escasa simpatía por Anonymous, un sentimiento que quedó claro en la frase final de su última publicación, a modo de brindis: «esto va por los dos años HTP, amigos. Recordad; relajaos, divertíos, sed los mejores y dosead a Anonymous nada más verlos.»[201]

¿Qué mejor manera de impresionar a un respetado grupo de hackers underground que detesta a Anonymous que sacrificando a Anons, algunos de los cuales son incluso amigos tuyos? (Más tarde, Cleary se retractó y, según tflow, estaba «celoso de LulzSec y trató desesperadamente de entrar en el grupo, que es la razón por la que ofreció su botnet».) Las pequeñas guerras libradas entre hackers han sido desde hace mucho tiempo un magnífico activo para las investigaciones llevadas a cabo por las autoridades del orden público. Como cabía prever, después del reprobable movimiento de Cleary, alguien que estaba lejanamente afiliado a Anonymous decidió a su vez dosearle. Nadie sabía a ciencia cierta si el nombre revelado era correcto, pero, como en el caso de Sabu, el tiempo se encargaría de demostrar que lo era. LulzSec, mencionado de manera explícita en el boletín de HTP, reflexionó sobre los recientes acontecimientos:

<Sabu>: pero necesitamos hacernos con ryan
<Sabu>: él dañó muy seriamente a anonymous con esto
<Falcon>: o algo
<lol>: bueno ahora tenemos su información
<Falcon>: su voz me molesta

El resto de los operadores de AnonOps, furiosos por lo que Cleary había hecho, transmitió una declaración disculpándose con la amplia comunidad de Anonymous y alentando a la gente a que se mantuviera alejada durante algún tiempo mientras ellos se ponían manos a la obra a montar un sistema más seguro. Este enfriamiento creó el escenario perfecto para que LulzSec se colocara bajo el incansable foco de los medios de comunicación.

LulzSec propiamente dicho

LulzSec zarpó con un cargamento compuesto por los datos volcados de la Fox, una cuenta de Twitter recién acuñada, y generosos memes y declaraciones de Internet absurdos, como queda ejemplificado en la justificación ofrecida cuando finalmente publicaron los datos de la Fox: «¿Sabéis a quién defendemos? A Common. Fox le ha llamado ‘despreciable rapero; nosotros llamamos a la Fox escoria común. ¿Creéis que hemos terminado? La diversión no ha hecho más que empezar.»[202] El equipo ya estaba acostumbrado a los ritmos y caprichos de cada uno de sus miembros. Habían formado una unión tan fuerte que, de hecho, todo el mundo sabía más o menos desde donde se estaban conectando los demás (aunque nunca compartían sus nombres auténticos). La mayoría residía en Reino Unido o cerca, excepto Sabu. Algunos de ellos incluso habían hablado ingenuamente a través de Skype, que fue como Topiary decidió que la voz de Cleary resultaba “irritante”.

OpSec, abreviatura de seguridad operativa, es el arte de proteger las interacciones humanas y digitales de tu grupo. Uno de los fundamentos de una buena OpSec es tener un cabal conocimiento del nivel de seguridad del ordenador y la red propios. La dependencia de paquetes de software comercial —opacos tanto en código fuente como en prácticas empresariales — puede comprometer ese conocimiento. El empleo de software libre, como GNU/Linux, y evitar el uso de herramientas como Skype (comúnmente percibida como un software con puertas traseras controladas por el gobierno) son medidas necesarias en el interminable recorrido de la siempre alerta OpSec. Mantener la información personal a nivel privado es también uno de los pilares fundamentales de OpSec. Si uno ofrece

voluntariamente esta información, no importa cuán seguros puedan ser su software y su hardware. Antes de llevar a cabo un ataque hacker hay que tener en cuenta todas estas consideraciones y más; cualquier otra cosa es estar pidiendo a gritos que te detengan. Con eso queremos decir que, con escasas excepciones, OpSec no era uno de los puntos más fuertes de LulzSec. De hecho, después de la avalancha final de arrestos de miembros del grupo, sus prácticas habrían de convertirse en un modelo, para otros hackers y activistas, de lo que *no* debe hacerse.

Pero estas preocupaciones quedaban muy lejos en el horizonte y el mar parecía un espacio enorme, incluso infinito. Durante el mes y medio siguiente, los logros de LulzSec demostrarían ser fascinantes. Se podría suponer que me estoy refiriendo a la creatividad técnica, pero, de hecho, con una pocas e inteligentes excepciones, los hackeos realizados por LulzSec eran más notables por su audacia y estilo que por su excelencia científica.

La verdadera importancia de LulzSec residía en su capacidad de forzar un reconocimiento y un debate más profundos sobre diversas cuestiones, desde el estado lamentable de la seguridad en Internet hasta el insaciable apetito del sensacionalismo mediático.

«Por qué amamos secretamente a LulzSec» (No tan secretamente, de hecho)

No todos los hackers albergaban sentimientos tiernos y cariñosos hacia Anonymous. Sus intervenciones eran a menudo demasiado poco sofisticadas a nivel técnico como para granjearse el respeto de la profesión. Algunos hackers pensaban que sus tácticas perjudicaban la causa mayor de la libertad en Internet, mientras que otros consideraban que sus payasadas eran pueriles. En fin, para otros, el estilo general del activismo perturbador, por muy interesante que pudiera parecer, simplemente no era lo que les gustaba. Pero con LulzSec era diferente. Un número sorprendente de hackers, especialmente los especializados en seguridad, adoraba al nuevo grupo, o al menos mostraba un ambiguo respeto hacia ellos. Para entender la razón, permitidme que ofrezca un retrato de este subgrupo de hackers relatando mi propia introducción en el modelo.

Antes del auge de LulzSec llegué a conocer la comunidad de seguridad de la información (InfoSec) de Nueva York, principalmente por causas de fuerza mayor. Aparentemente había ofendido a algunos hackers de seguridad al consagrar como hackers, por escrito, a desarrolladores de código abierto, programadores que liberan su código fuente con licencias permisivas –como los hackers. A consecuencia de semejante "error" degradante, los investigadores especializados en cuestiones de seguridad, que también se llaman a sí mismos hackers, se pusieron en contacto conmigo apelando a diversos medios, desde sugerencias constructivas e invitaciones a debates hasta burlas espeluznantes y amenazas intimidatorias. Su intención era instruirme sobre lo que eran los "verdaderos" hackers: ellos mismos. ¿Cree que un ordenador DIY, un trasto controlado a distancia y que funciona en un ordenador de código abierto de veinticinco dólares llamado Raspberry Pi, constituye hackeo? No, lo siento. ¿O qué me dice de programar LED *throwies* de luz parpadeante que luego tiene intención de repartir en una *rave*? Otra vez, no. Estos pueden ser artilugios molones y útiles que requieren cierta capacidad técnica —y no hay duda de que podrían ser parpadeantes— pero no constituyen un HACKEO. El hackeo, me dijeron, es invasión digital: penetrar en un sistema, dominarlo por completo, hacer lo que quieras con él. Yo acababa de publicar poco tiempo antes mi libro sobre los "hackers" de software libre *Coding Freedom: The Ethics y Aesthetics of Hacking* y daba la impresión de que estos guerreros de la palabra reunidos alrededor de la seguridad de la información pensaban que tenía una visión estrecha del término en cuestión, un enfoque que pasaba por alto su mundo. Pero mi comprensión del término está mucho más matizada de lo que ellos entendían. Mi definición incluye a programadores de software libre, a personas que hacen cosas y *también* a personas que comprometen los sistemas, pero eso no significa que haya que hablar sobre ellos todo el tiempo. Mi primer libro tenía un enfoque específico.

Resulta interesante señalar que, mientras que cada microcomunidad reivindica el apelativo "hacker", algunos de ellos refutan siempre los intentos de otras microcomunidades de reivindicar ese término. De modo que, cuando la gente de seguridad de la información empezó a gritarme que los "hackers" de software libre no eran "hackers", no me sorprendí en absoluto. De hecho valoré mucho más los debates productivos generados

alrededor de esa cuestión, que las amenazas veladas.

En algún momento en 2010 recibí un correo electrónico de un respetado hacker en el que me animaba a asistir a la NYSEC, una reunión informal de profesionales de seguridad y hackers que se celebra todos los meses en un bar de Nueva York. O tal como la describe su perfil de Twitter, «un encuentro entre copas con un problema de seguridad de la información». Pensé, ¿por qué no? Era una manera cordial de decirme: *frecuenta la realidad, empieza a salir con auténticos hackers*. Otros no fueron tan amables. Uno de estos “hackers” se puso en contacto conmigo por correo electrónico para ofrecerme generosamente toda su colección de *2600*, la revista de los hackers, para mi investigación. Estaba emocionada por la posibilidad de añadir estas publicaciones a mi biblioteca personal y nos encontramos en un diminuto café de Nueva York. Después de abordar el tema de mi libro se empezó a poner nervioso y dijo, entre resoplidos, que «configurar Linux no es hackear». Este caballero, que tenía probablemente unos cuarenta y cinco años, estaba tan alterado que se levantó y se marchó del café. Una actitud amable, comparada con la vez en que un hacker me encontró online y me advirtió que acababa de ver cómo un montón de hackers estaba conspirando en el IRC para hackear mi ordenador y darme una lección sobre lo que hacen los verdaderos hackers. Nada como un hackeo *in situ* para ponerte en tu lugar. Asustada, cerré todos mis sistemas para estar segura y sospecho que el conocido que me aconsejó que lo hiciera pudo haber convencido a los celosos hackers de que se calmaran.

Naturalmente, no todos los hackers de seguridad se oponen tan diametralmente a extender esa etiqueta a los desarrolladores de software libre/de código abierto. Muchos hackers que tratan con cuestiones de seguridad utilizan y escriben ellos mismos el software de código abierto. Uno de esos hackers, David Mirza, residente en Montreal, ha pasado un montón de horas instruyéndome acerca de las complicadas estética y política del hacker underground. Mirza, que había pertenecido al ambiente de los sombreros negros, dirige actualmente una empresa de seguridad informática y es un infatigable defensor del software de código abierto.

Pero existen diferencias, algunas importantes. Muchos de estos hackers que trabajan como contratistas, o en el ámbito de la seguridad para gobiernos o empresas, se enfrentan continuamente a enormes desafíos cuando se trata de asegurar aplicaciones informáticas, sistemas operativos,

servidores y sistemas que trabajan en línea. Asegurar realmente un sistema significa, como mínimo, invadir la forma de pensar de cada posible infiltrado. A menudo, eso significa participar uno mismo en la intrusión. Ésta es la razón por la que muchos de los mejores hackers de seguridad son antiguos sombreros negros que aún pueden, ocasionalmente, implicarse en este tipo de actividades que se encuentran en una zona de ambigüedad legal. Los hackers de seguridad informática tienden a ser un tanto paranoicos y no es de extrañar que así sea. Tú también lo serías si pasaras la mayor parte de tus horas de vigilia perfeccionando tus propias capacidades de intrusión mientras, al mismo tiempo, ahuyentas a estafadores de tarjetas de crédito, socios de redes rusas de negocios, creadores de virus búlgaros, hackers estatales chinos y los tropecientos villanos más que buscan activamente acceder a sistemas valiosos. Los hackers que se encargan de garantizar la seguridad soportan la carga de la paranoia para que el resto de los mortales podamos dormir un poco mejor por las noches. (Pero no durmáis demasiado profundamente; su consejo no siempre es atendido.)

Cualquiera que haya tenido trato con hackers sabe que, cuando se trata de la tecnología, los hackers de todas clases son unos esnobs insoportables. Esta actitud no es privativa de los hackers de seguridad frente a los evangelistas del software libre, ni tampoco es privativa de los hackers en términos más generales. La arrogancia vocacional es común a todos los artesanos: médicos, profesores, académicos, periodistas y fabricantes de muebles. Es simple: el buen arte de la soberbia nos impulsa a hacerlo mejor. Sin embargo (y por razones que, en gran parte, se me siguen escapando), cuando se lo compara con otras actividades que también se podrían considerar “hackeo”, los especialistas en seguridad llevan el elitismo a niveles incomparables. Los elogios no salen fácilmente de los labios de estos hombres y mujeres dedicados a la seguridad en la información.

Si combinamos esta imagen simplificada con el reconocimiento del escarnio histórico de Anonymous por parte de InfoSec podemos apreciar mejor por qué la adoración que le profesa a LulzSec la comunidad de seguridad es mucho más notable. La siguiente fotografía tomada durante la celebración de Halloween en ٢٠١١ podría ser lo que mejor lo resume:[203]



Disfrazados de LulzSec, estos hackers residentes en Nueva York no solo estaban viviendo a lo grande y pasándoselo de maravilla, sino que también mostraban todo su apoyo a los hackers inadaptados y rebeldes. Si bien están representadas todas las características de la mitología LulzSec, hay un elemento adicional que quizás no resulte tan obvio: la ausencia de pantalones. Muchos consideraron que LulzSec estaba señalando, en el agresivo estilo de Internet, el hecho de que el *Emperador va desnudo*. Desde siempre, los profesionales en seguridad han estado reclamando a gritos desde lo alto de una montaña solitaria, yerma y barrida por el viento, la necesidad imperiosa de que las organizaciones inviertan más recursos, energía, tiempo y personal en mejorar la seguridad. LulzSec, al parecer, había encontrado al fin una manera de hacerse escuchar.

Cabría preguntarse por qué la seguridad es tan deficiente en un sector tan amplio y rentable. Después de todo, el (ciber-)miedo vende.[204] La industria no solo vende regularmente estafas informáticas (tales como creativas soluciones informáticas imposibles de configurar para abordar los perfiles de riesgo propios de una institución) o productos cuya finalidad es sustituir a un equipo de seguridad específico que puede hacer más mal que bien, sino que el deseo inicial por la propia seguridad sigue teniendo una prioridad muy baja para muchas empresas, incluso aquellas que cuentan con una excelente financiación. Un hacker de seguridad de Nueva York me explicó: «Uno de los desafíos de la seguridad es conseguir que la gente se la tome en serio, porque a nivel ejecutivo solo se percibe como un gasto.» El hecho de que en 2011 se hubiera podido saquear a Sony —una empresa multinacional—con semejante impunidad es un claro indicio de la profundidad y naturaleza de los problemas. Este tipo de casos son los que hacen enfurecer a los hackers que crean sistemas seguros.

LulzSec, más que cualquier otro informe, persona o grupo en la historia reciente, consiguió transmitir un mensaje que muchos profesionales en el ámbito de la seguridad habían estado lanzando durante más de dos décadas sin ningún éxito. Los efectos fueron similares a las payasadas antagónicas de L0pht Heavy Industries, una asociación informal de hackers cuyos miembros mantenían regularmente reuniones presenciales. In 1998, durante una conversación de grupo, un par de ellos acuñó el término “sombrero gris” para describir a aquellos hackers que se sitúan ambigua y deliberadamente entre las etiquetas blanca y negra que han llegado a diferenciar a los hackers maliciosos de los más benévolos. Los hackers de “sombrero gris” no están por encima de las actuaciones ilegales, pero habitualmente solo actúan para detectar, y divulgar, vulnerabilidades. L0pht tuvo tanto éxito que, en mayo de 1998, siete de sus miembros fueron invitados a testificar (de un modo un poco teatral) ante el Comité de Asuntos Gubernamentales del Senado, presidido por el senador republicano Thompson. Con su refinado, sombrío y fuerte acento de Tennessee, el senador Thompson presentó al “*think tank* de hackers” y explicó que «debido a la sensibilidad del trabajo realizado en L0pht, utilizarán sus apodos de hacker: Mudge, Weld, Brian Oblivion, Kingpin, Space Rogue, Tan y Stefan».[205] Un coro de risas apagadas atravesó las salas, probablemente porque esos apodos eran superfluos: la cadena C-SPAN había grabado los testimonios y los hackers habían sido desenmascarados. Sus comentarios abordaron numerosos temas, pero la afirmación de que podían desactivar Internet en treinta minutos destacó sobre las demás. No se trataba de una amenaza, sino que fue casi una súplica para que se mejorase el terrible estado en el que se encontraba la seguridad de Internet en 1998.

El testimonio de los integrantes de L0pht ante el Senado de los Estados Unidos fue respetuoso; muchos de los participantes llevaban traje y se hizo un visible esfuerzo por dar explicaciones que fueran ampliamente comprensibles. LulzSec no fue invitado a visitar el Congreso —ni tampoco pudieron desactivar Internet— pero en el curso de su búsqueda errante consiguieron transmitir un mensaje similar. Hicieron que la gente prestase atención al sórdido estado de la seguridad en la red, no ofreciendo un testimonio cuidadosamente elaborado sino a través del simple itinerario de sus viajes en busca de aventuras (que casualmente incluyó más de una docena de hackeos de perfil alto). Lo hicieron a la luz de las leyes

estadounidenses, como la CFAA, que se concibieron para castigar a cualquier hacker que fuese atrapado, independientemente de su motivación. Los desafiantes hackeos de LulzSec contra gigantes corporativos y organismos del gobierno, que hoy es material de leyenda, fueron muy eficaces —tal vez hasta necesarios— para que la gente despertase.

Muchos expertos en seguridad a los que entrevisté citaron directamente el papel de LulzSec a la hora de conseguir que ejecutivos de alto nivel prestasen atención a sus mensajes, al menos durante un breve período (2013 fue testigo de una cadena de filtraciones masivas de datos: Adobe, Target, Neiman Marcus, LivingSocial, la Oficina Administrativa de los Tribunales del Estado de Washington, Evernote, Drupal.org, la Reserva Federal de los Estados Unidos, OKCupid..., la lista es interminable).[206] En 2011, una entrada en el blog de Patrick Gray, periodista e investigador sobre seguridad, titulada "Por qué amamos secretamente a LulzSec", fue ampliamente leído por los profesionales en seguridad y captó muy bien el espíritu que reinaba entre ellos. Gray me explicó el impacto que había tenido su texto: «Hizo más ruido que cualquier otra cosa que hubiera escrito antes, incluidos textos para ZDNet/CNet, *The Sydney Morning Herald*, *The Age*, *Wired*... He escrito un montón de artículos sobre noticias que trascendieron a nivel mundial, pero esto fue algo completamente diferente.» En el artículo, Gray escribió:

> Podría resultar sorprendente para los observadores externos, pero los profesionales en seguridad también se lo están pasando secretamente en grande al observar cómo estos tíos se vuelven locos... Los principales medios de comunicación se divierten criticando a Sony por su deficiente seguridad, pero, ¿pensamos sinceramente por un segundo que la red XBox Live no puede ser atacada de la misa manera? (Sé que la infiltración en la PSN no ha sido atribuida a LulzSec, pero el problema no ha desaparecido.) ¿Existe algún objetivo allí fuera que no pueda ser "conseguido"?[207]

Si bien los innumerables problemas de seguridad que afectan a Internet no podían solucionarse por arte de magia, seguía siendo gratificante desafiar al problema más obvio, como lo describió Gray.

El espectáculo ofrecido por LulzSec reveló asimismo la hipócrita farsa

de muchas empresas mientras realizaban extrañas contorsiones para quitarse la culpa de encima. Un investigador de seguridad residente en Nueva York que prefiere mantener el anonimato explicó:

> Una cosa que considero interesante es que esta gente [las corporaciones] está siendo atacada todos los días, pero su información no se distribuye por Internet. Habitualmente la gente se apropia de esa información para obtener un beneficio. La ironía es que cuando la gente roba propiedad intelectual para conseguir un rendimiento financiero, no se haga nada al respecto... Creo que es algo irónico, ahora que LulzSec está haciendo que la gente cuide de sí misma.

Esta postura fue reflejada también por Chris Wysopal, uno de los miembros originales de L0pht, que ahora dirige una respetada empresa de seguridad:

> Las corporaciones se toman más seriamente la vergüenza pública que la propiedad intelectual robada. Los ataques a Sony provocaron escalofríos a los CISO (directores de seguridad de la información) de Fortune 100 y a sus juntas directivas. Teníamos clientes que venían y nos decían literalmente, «No quiero ser otro Sony». Escanearon miles de sitios web y solucionaron centenares de vulnerabilidades críticas para que no les ocurriera lo mismo. De este modo, LulzSec consiguió que Internet fuese más resistente. En cierta manera es como una vacuna que facilita a tu sistema inmunitario una muestra del virus que, de otro modo, te mataría, y obliga a que tu sistema inmunitario trabaje para crear una protección contra ese virus.

La popularidad de LulzSec entre el personal de seguridad excedió su función práctica de obligar a los ejecutivos a «cuidar de ellos mismos». Su vocabulario rico pero accesible encarnaba el placer mágico y subversivo del hackeo, mantenido invisible con mucha frecuencia. Se puede pensar que hacer o vulnerar, explotar o construir, asegurar y evaluar no pueden incluir talento artístico, expresión creativa y placer, pero esto es exactamente lo que experimentan estos tecnólogos: placer (junto con esa clase de frustración desesperante que hace que el placer sea el doble de potente al superarla). Transmitir la naturaleza de esta satisfacción a los outsiders es

prácticamente imposible porque la destreza técnica es demasiado hermética. Las bufonadas divulgadas de LulzSec constituyen la representación más precisa que he visto nunca de la imagen, el ambiente y las sensibilidades que intervienen en los placeres del hackeo. Y cada pieza de la iconografía de LulzSec simboliza los aspectos sensuales e ideológicos de este mundo: el barco (que representa la libertad de los piratas en alta mar), el hombre con traje y monóculo (el hacker snooty l33t), el gato (porque si está relacionado con Internet debe haber felinos), la música (hackear con música siempre es preferible a hacerlo en silencio), los manifiestos (libertad de expresión, ¡joder!) e infringir la ley (porque, las reglas, que se vayan a la mierda). LulzSec encarnaba el placer del hackeo y la subversión como ningún otro grupo. LulzSec representaba también un sitio de anhelo y fantasía. Lo que el grupo hacía de un modo tan descarado era algo que muchos hackers *deseaban* hacer. Algunos de ellos habían experimentado sin duda los mismos placeres ilícitos en el pasado, cuando el mundo de la informática se abrió a ellos por primera vez a través de la exploración y el entretenimiento, pero aquello era algo que se hacía habitualmente sin contar con una audiencia masiva a nivel mundial.

Ahora bien, no todos los hackers adoraban a esa tripulación. HTP, el grupo que adoraba atacar a Anonymous, extendió su desprecio a LulzSec. Tal como lo expresó un miembro de LulzSec que respondía al nombre de pwnsauce, «HTP nos veía básicamente como a una panda de inútiles que nos prostituíamos buscando llamar la atención». El punto de vista de HTP refleja una ética de larga fecha en el mundo de los hackers underground, una ética que lleva a algunos hackers a despreciar a aquellos que buscan llamar la atención de los principales medios de comunicación (la atención es un anatema para mantenerse alejado de la “cárcel” y el fracaso de LulzSec demostró la sabiduría de esta ética popular). Si bien los hackers de LulzSec no concedieron muchas entrevistas, estaban haciendo todo lo posible para ser noticia, atrayendo sobre ellos la mayor atención posible. En una ocasión lo hicieron atacando a los propios medios de comunicación.

Los medios de comunicación

Es posible que Anonymous no haya designado nunca (fácilmente) a ningún

individuo para que hablase en su nombre, pero contaba con un canal de IRC, #reporter, donde docenas de periodistas entrevistaban a los participantes. LulzSec era más reservado, no ofrecía ningún canal público para el acceso periodístico y, en general, no concedía prácticamente ninguna entrevista (excepto a Parmy Olson y, alguna vez, a Steve Ragan). No había ningún famoso al que exhibir, excepto el propio grupo. No obstante, hacia finales de junio de 2011, LulzSec se había convertido en algo similar a un grupo de estrellas de rock. Esta incursión en el territorio de las celebridades provocó cierta contrariedad en la amplia comunidad de Anonymous pero, en su mayoría, existía la distancia suficiente —LulzSec insistió en confirmar su autonomía— para que incluso los colectivos con seudónimo de los que LulzSec se había separado pudieran disfrutar del espectáculo sin sentir que eso afectaba a sus propia costumbres y sensibilidades éticas.

LulzSec, a diferencia de AnonOps, clavó las uñas en los medios de comunicación. Su mayor hackeo contra la prensa tuvo como objetivo el PBS (Servicio Público de Divulgación) como represalia por su película de Frontline sobre WikiLeaks, *WikiSecrets*. El documental provocó la ira de los miembros de LulzSec, principalmente de Sabu, a quien la película no le gustó en absoluto por la forma en que eludía las apremiantes cuestiones políticas suscitadas por el Cablegate en favor de un psicoanálisis sensacionalista de la "oscura" vida íntima de Chelsea Manning. LulzSec lanzó una doble campaña. Descargaron los datos personales de la plantilla de PBS y desfiguraron su sitio web, dejando un artículo ingenioso que *casi* podía pasar como auténtico (*véase* la figura en la página siguiente).

Aunque el artículo estaba destinado (y diseñado) para que se percibiera como falso, funcionó como un montaje. Tal vez debido a que el escenario era verosímil en términos hipotéticos, Topiary (su redactor) salpimentó el artículo con revelaciones involuntarias. La fuente de información presentada —un diario manuscrito— era absurdo y pintoresco para los estándares actuales. Y el dato más increíble era la sugerencia de que las autoridades policiales estaban en el asunto, no solo porque la privacidad escasea para las celebridades sino porque la privacidad en sí misma ha sido inexistente durante mucho tiempo. En caso de que hayas sido engañado, el pateador de la historia te devuelve a la realidad con la absurda afirmación de que «arranca como un obituario vital» (un anagrama de los handles de los miembros de LulzSec que participaron en el hackeo, Topiary, Sabu,

Kayla, Avunit) y una referencia a la novia del autor del diario, Penny, llamada nada menos que como la presidenta de HBGary.

Si bien algunos se sintieron molestos por un ataque dirigido contra los medios de comunicación, la locura desatada en Twitter cuando se divulgó la historia mostró, en su inmensa mayoría, adulación. El encanto de esta acción se puede explicar si recurrimos a una definición antropológica de desconfiguración aportada en el impresionante libro de Michael Taussig sobre el tema: «la desfiguración actúa en los objetos del mismo modo en que las bromas lo hacen en el lenguaje, exhibiendo su magia inherente, sobre todo cuando esos objetos se han convertido en rutinarios.»[208] LulzSec puso al descubierto el tema de la celebridad desfigurando un objeto mediático —el artículo periodístico— con una fuerte dosis de humor.

Todas las agencias principales de noticias occidentales publicaron notas sobre el falso artículo y la mayoría de ellas se concentró en la parte relativa a la éticamente cuestionable filtración de datos. La motivación política detrás del hackeo solo fue objeto de un tratamiento superficial, aunque LulzSec publicó una declaración explícita razonando sus acciones. Fue una nueva (e irónica) demostración de la proclividad de los medios de comunicación dominantes a destacar la parte sensacionalista de las noticias, la misma conducta mostrada con el documental sobre WikiLeaks que provocó la operación en primer lugar.


PBS NEWSHOUR

Topics | Video | Recent Programs | Teacher Resources

The Rundown — A BLOG OF NEWS AND INSIGHT

TUPAC -- May 29, 2011 at 11:30 PM EST

TUPAC ESTÁ VIVO EN NUEVA ZELANDA

El famoso rapero Tupac ha sido hallado con vida y en buen estado de salud en un complejo de vacaciones de Nueva Zelanda, según fuentes locales. El pequeño pueblo —cuyo nombre no se menciona debido a los riesgos para la seguridad —albergó supuestamente a Tupac





y Biggie Smalls (otro rapero) durante varios años. Uno de los habitantes locales, David File, falleció recientemente y dejó pruebas e informes de la visita de Tupac en un diario, que pidió que se enviara a su familia en los Estados Unidos.

«Nos quedamos sorprendidos al ver lo que David había dejado –dijo una de sus hermanas, Jasmine, de 31 años–. Pensamos que lo mejor era que el mundo lo supiera, ya que creemos que este material no merece ser mantenido en secreto.»

David, de 28 años, fue víctima recientemente de un tiroteo desde un coche por parte de conocidos gánsteres locales. A raíz de los numerosos impactos de bala recibidos cuando se dirigía a su casa desde el trabajo, David fue declarado muerto en el lugar de los hechos. La policía encontró el diario en un cajón de su mesilla de noche.

«Naturalmente no leímos el diario –afirma uno de los oficiales–. Simplemente tomamos nota de la petición de que se enviara a una dirección en Estados Unidos, lo que hicimos para respetar la voluntad de David.»

Los agentes de policía han cerrado las carreteras al pueblo y no harán especulaciones sobre si Tupac o Biggie han sido trasladados a otra región u otro país. Los habitantes locales se niegan a comentar exactamente cuánto tiempo o por qué estuvieron refugiados allí; un hombre se limitó a manifestar «aquí no hablamos de eso».

Desde entonces, la familia de David File ha solicitado que se tomen más medidas para arrestar a los responsables del tiroteo. «David era un chico inocente y encantador –declaró su madre–. Nunca había sido tan feliz como cuando se trasladó a Nueva Zelanda.»

Su hermano Jason pidió que se hiciera pública una parte del diario de David en un intento de descifrarlo. «Cerca del final –dice Jason– hay una línea en la que se lee 'arranca como un obituario vital', que hasta ahora no hemos sido capaces de entender.»

La novia de David, Penny, no quiso hacer ninguna declaración.

«Escaneamos el futuro»

Uno podría pensar que la respuesta corporativa a LulzSec, y por extensión a Anonymous, había sido absolutamente negativa. En realidad, fue un poco más complicado. Comenzando en el otoño de 2011 y alcanzando su punto álgido en 2012, numerosos individuos e instituciones situados en la cima del mundo empresarial y cerca de ella comenzaron a ponerse en contacto conmigo. Hablé con el socio fundador de una firma de capital de riesgo de Nueva York, con el director de seguridad europea para Vodafone y con un vicepresidente sénior de TTI/ Vanguard (descrito como «un foro exclusivo

para ejecutivos de nivel superior que vincula la planificación de tecnología estratégica con el éxito empresarial»). Di un par de charlas (una virtual) para un grupo mundial de seguridad y riesgo con sede en Nueva York que incluyó a oficiales jefes de seguridad (CSO) y otros ejecutivos de importantes corporaciones. Por último, participé en un evento dirigido por World 50, una organización que organiza eventos para ejecutivos de alto nivel, principalmente de las empresas de Fortune 500.

La lista estaría incompleta si no mencionamos mi conferencia de 2012 en el TEDGlobal en Edimburgo, Escocia. Mientras que los vídeos en línea de TED alcanzan una audiencia popular de millones de personas, la conferencia en sí cuenta con la asistencia de élites adineradas, con la excepción de algunos ponentes, como es mi caso, y selectos participantes que reciben ayuda financiera de TED. El privilegio de asistir a TED cuesta aproximadamente seis mil dólares. Por supuesto, a uno tienen que elegirlo primero (tienes que presentar una solicitud). Esta suma no incluye los gastos de viaje o alojamiento, pero garantiza el acceso a fiestas elegantes que incluyen abundante comida y bebida, conciertos, conferencias TED de alto nivel y la oportunidad de entablar conversación con algunas personas célebres y fascinantes (o, al menos, con sus asistentes). Tras mi intervención, el asistente personal de Will Smith entabló una conversación conmigo, durante la cual hizo un intenso esfuerzo para convencerme de que su jefe, de quien se rumorea que es cienciólogo, es en realidad un ferviente simpatizante de Anonymous. ¿Estaba sometiéndome a una sesión de ingeniería social para proteger a su jefe de un ataque de Anonymous potencialmente nocivo para su carrera, o en realidad nos habíamos topado por casualidad en medio de la fiesta?

Aquello fue bastante normal comparado con otro encuentro memorable que tuve en aquella ocasión. Mientras degustaba los deliciosos canapés durante uno de los descansos, un ejecutivo de una empresa de la lista Fortune 500 se me acercó, me tomó del brazo —con una presión excesiva, pensé— y, proyectando claramente su ansiedad sobre mí, me susurró ruidosamente al oído: «Es usted *taaaaaaaan* valiente por estudiar a Anonymous.» Apenas el día anterior había visitado a un Anon y a su compañera. El momento culminante del día fue el paseo por su jardín, donde admiré su colmena, seguido de una muy sabrosa comida casera compuesta de faisán y puré de boniato. Después vimos el documental *We*

Are Legion: The Story of the Hacktivists y su compañera se sintió bastante abrumada al darse cuenta de que, en realidad, en Anonymous había cierta sustancia política. Durante todo ese tiempo había estado convencida de que su novio había jugado en su ordenador y participado en acciones puramente juveniles. Después de esta agradable experiencia con un "temido" Anon, me resultó difícil fundirme ante las alabanzas de valentía y coraje de este ejecutivo. *Creo que podría haber soportado la picada de una abeja*, pensé para mí.

A un determinado nivel, estos hombres y mujeres me parecieron gente corriente. Se quejaban de sus hijos e hijas malcriados, del exorbitado coste de la educación superior en Estados Unidos y (algunos de ellos, al menos; un canadiense nacionalizado, ahora que lo recuerdo) de la falta de una asistencia sanitaria universal en Estados Unidos. Muchos incluso participaban en un pasatiempo tradicional en sus lugares de trabajo: criticar a su superior inmediato. En este medio, por supuesto, ese suele ser el consejero delegado de una megaempresa. Pero no nos confundamos: durante el evento World 50 celebrado en el Contemporary Jewish Museum de San Francisco, escuché a dos jóvenes encargados del servicio de catering murmurar entre ellos, sin que les importara que pudiese oírles claramente, que «lo que hay ahí dentro es un mundo diferente». Tomemos, por ejemplo, las tarjetas de identificación que nos habían entregado a los asistentes al evento. No eran una simple-cartulina-cubierta-con-una-funda-de-plástico-con-alguna-clase-de-cordones-con-la-imagen-corporativa. Parecían haber salido directamente de una tienda de muebles de diseño. El cierre, metálico, estaba alimentado por un imán. En caso de apuro lo podías utilizar como un arma ninja. Lamentablemente, la mía solo la utilicé para identificarme. Después de conseguir mi tarjeta de identificación y de un almuerzo de atún ahumado y otros manjares, nos hicieron subir a un salón privado espacioso y soleado, engalanado con sillas de felpa para las charlas, cuyos temas iban desde cursos en línea masivos y abiertos (o MOOC) hasta Anonymous (el mío, por supuesto). Entre el público había ejecutivos de AstraZeneca, Cargill, Hewlett-Packard, Hilton Worldwide, Huawei Technologies, Hyatt Hotels, Juniper Networks, Monsanto, Río Tinto, Coca-Cola Company y Tiffany&Co. Aunque habíamos almorzado hacía unos minutos, había una impresionante oferta de bocadillos y bebidas, incluidas hermosas copas llenas de M&M y diez tipos distintos de bebida. Una vez acabadas las

charlas nos llevaron a todos a disfrutar de la cena en un restaurante que dominaba el famoso Bay Bridge y que comenzó con un monólogo íntimo a cargo de Steve Martin.

No debe sorprender que los ejecutivos de las grandes corporaciones, especialmente los pertenecientes a las empresas líderes, desearan por encima de todo que alguien agitara una varita mágica e hiciera desaparecer tanto a Anonymous como a LulzSec. Los ejecutivos de las empresas tecnológicas parecían curiosos y al menos familiarizados con la implicación de Anonymous en una serie de movimientos políticos. En ocasiones incluso se mostraban interesados en conocer cuál había sido el papel de Anonymous en los sucesos de la Primavera árabe. Los ejecutivos de las empresas financieras y energéticas tendían a ser glaciales, mientras que otros procedentes de otras industrias mostraban una curiosa combinación de disgusto y temor. La directora de comunicaciones de una compañía aérea low-cost bromeó, deseando que Anonymous hackeara su empresa. La publicidad gratuita en ese caso sería espectacular.

Pero lo que menos esperaba fue una consulta que recibí sobre la posible contribución de Anonymous al mundo corporativo. TTI/Vanguard se me acercó para evaluar si podía dar una charla de esta naturaleza a sus clientes, tales como Royal Dutch Shell, Northrop Grumman, Toyota, FedEx y Expedia. Fue entonces cuando descubrí que TTI/Vanguard se dedicaba fundamentalmente a “escanear el futuro”. Aparentemente, «TTI/Vanguard refuerza el pensamiento relativo a las posibilidades tecnológicas. Escaneamos el futuro. Nos centramos en las fuentes de cambio imprevistas y evaluamos su promesa transformadora. Mediante sesiones dinámicas y altamente interactivas se estimula el debate y prosperan las ideas innovadora.»[209]

Ésta es la cultura que adopta estrategias “perturbadoras” para la economía de la atención, para la plusvalía. Anonymous y LulzSec eran elementos perturbadores a la manera clásica, sin ninguna aclaración. En ocasiones incluso creaban el caos solo como diversión. Demostraron también la importancia del arte, la expresión, la autonomía y la creación a través del trabajo no alienado. La mayoría de las empresas multinacionales no son compatibles con estos ideales; no pueden aplicar estas lecciones, no al menos de una manera honesta y gratificante.

La misión de la declaración de TTI/Vanguard señaló mi primera

exposición al “escaneo del futuro”, pero luego comenzó a aparecer en todas partes. La situación más sorprendente con este grupo se produjo durante una conversación telefónica con Chris Anderson, el jefe de TED, previa a la celebración del evento de aquel verano en Edimburgo. Anderson me preguntó si mi charla podía incluir algunas ideas prácticas para la gestión empresarial. Aunque su petición no carecía de sutileza, estaba claro que deseaba que impartiera una clase (eminentemente inspiradora, asombrosa, perturbadora) desde las trincheras de Anonymous, capaz de cambiar totalmente la sabiduría convencional y estimular el pensamiento corporativo. Hasta entonces había trabajado principalmente con el otro comisario de TED, Bruno Giussani. TED lo revisa todo hasta la última palabra; Bruno me pidió que quitase la palabra “patria” ya que tenía una connotación política excesiva. Dicho esto, Giussani era por otra parte un tipo discreto que me ofrecía sugerencias útiles que yo podía aceptar o rechazar. Honestamente, la consulta de Anderson me sorprendió. Resultaba evidente que si adoptaba el léxico corporativo y les proponía alguna forma hábil de envasar a Anonymous mediante frases superficiales, impresionantes, que cambiasen el paradigma y combinadas con un confuso balbuceo tecnológico, todo ello transmitido con un entusiasmo jadeante, daría con la fórmula perfecta para inspirar en estos drones corporativos la sensación de que estaban asistiendo a unas reflexiones alucinantes. Entonces podría ganar un montón de pasta viajando y contándole mentiras a la gente hasta que apareciera el siguiente paradigma.

Estos intercambios me dieron una perspectiva fresca sobre un vector contemporáneo de implicación. Los académicos que escriben sobre este tema lo han enfocado con frecuencia desde los ángulos de la publicidad, el entretenimiento y el consumismo, siendo el ejemplo clásico en este sentido el análisis trascendental que hace Dick Hebdige de la mercantilización del punk rock.[210] Las fuerzas contraculturales de la crítica, de las que el punk rock era emblemático, son desnaturalizadas cuando se canalizan a través del aparato publicitario corporativo, o se convierten en mercancías mediante los mecanismos de procesamiento de Hollywood o de la industria de la moda. Lo que siempre me ha parecido interesante de Anonymous era cómo había resistido, al menos hasta hace poco,[211] a estas fuerzas por una razón fundamental: la mayoría de las corporaciones se muestran cautelosas a la hora de mercantilizar a Anonymous porque saben lo directas que podrían

ser las repercusiones. De hecho, el de Anonymous es un caso curioso en el que a menudo se produce el proceso contrario: si bien es verdad que Time Warner se lucra cada vez que alguien compra una máscara oficial de Guy Fawkes (Time Warner tiene el copyright de la película *V de Vendetta*), Anonymous ha adoptado un símbolo popularizado por Hollywood y lo ha convertido en revolucionario. Es un excelente ejemplo de contramercantilización, un fenómeno poco frecuente.

Pero si hay una lección que he aprendido de los ejecutivos corporativos, es ésta: si bien ellos no están a punto de reclamar las imágenes de Anonymous para su próxima campaña publicitaria, eso no significa que no puedan, o no quieran, encontrar alguna manera de apropiarse de *algo* sobre Anonymous. Si alguien es capaz de encontrar una idea no exprimida, explotable, escaneada en el futuro, innovadora y rompedora que puede prosperar en las salas de juntas de las corporaciones, lo harán. Este movimiento, aunque diferente de formas de implicación más familiares —ya que la transferencia de conocimiento puede no alterar (necesariamente) el fenómeno analizado— merece ser entendido un poco mejor. Existe una extendida industria artesanal (en forma de *think tanks*, organizaciones y conferenciantes motivacionales, muchos procedentes del área académica, especialmente expertos a los que les encanta exagerar la promesa de la tecnología) que funciona para capturar el saber en todos los rincones del globo (desde la cultura pandillera hasta la Primavera árabe) y transformarlo en una fórmula para alcanzar el éxito corporativo. Esto se lleva a cabo con el propósito de que los ejecutivos puedan mantenerse al día de los desafíos mundiales, sentirse de maravilla con lo que hacen, fortalecer la maquinaria cultural corporativa y ganar un montón de pasta con una cultura en la que no tienen que invertir. Sospecho que en algunos casos los ejecutivos corporativos que profundizan en un fenómeno como el código abierto no solo cosechan ideas para sus organizaciones, sino que tienen el poder de modificar la opinión pública sobre esa cuestión. Es muy poco lo que sabemos sobre el alcance de estas redes y los posibles efectos que el “escaneo del futuro” podría añadir. Es un tema que sin duda convendría conocer mejor. Tal vez necesitemos “escanear el futuro” escaneándonos el futuro a nosotros mismos.

«Yo os digo: todavía se debe tener caos en uno mismo para poder dar a luz a una estrella del baile»

LulzSec no solo era acogido y festejado por los hackers. También era muy popular entre los geeks de Internet, los activistas políticos y los académicos, junto a una multitud de otros espectadores camuflados. Para entender el porqué, puede ayudar si recurrimos al filósofo alemán del siglo XIX Friedrich Nietzsche, cuyas inversiones en cuestionar la verdad y la moral, elevar el placer por encima de la razón y adoptar el ingenio y la hipérbole pueden utilizarse (lúdica y experimentalmente) para crear el andamiaje intelectual del trabajo que LulzSec y Anonymous llevaron a cabo 150 años más tarde. (De hecho, si Nietzsche se hubiese teletransportado al futuro y hubiera desarrollado una afición por el hackeo, sospecho que podría haberse unido a las filas de LulzSec.)

Nietzsche se tomó tan seriamente el proyecto de la crítica de la Ilustración que resultó ser uno de sus críticos más infatigables, contribuyendo así a inaugurar un proyecto más amplio de filosofía radical, que una serie de escritores se encargaría de ampliar en el siglo XX, principalmente Gilles Deleuze, Félix Guattari y Michel Foucault. Podríamos incluso pensar en Nietzsche como el embaucador de la Ilustración. Los objetos de su crítica eran la racionalidad, el progreso, Dios, la ciencia y el modo en que las ideas o los sistemas basados en tropos absolutistas —ya sea que proclamen la verdad en la ciencia o en Dios— se vuelven, al obtener una adopción más extensa, más resistentes a la crítica y más capaces de tener a los seres humanos bajo control. Para Nietzsche nada debe concederse de facto ni asumirse a priori: ni el bien y el mal, ni lo verdadero ni lo falso. Cada fragmento de conocimiento que los seres humanos conciben, crean o incluso descubren a través de la observación del mundo es, según Nietzsche, provisional, está arraigado en el juicio y, aunque a menudo parezca intemporal o natural, solo es comprensible en un momento histórico específico.

El objetivo de Nietzsche era desmantelar el bastión ideológico de verdad, racionalidad y sistemas morales convencionales por razones complejas. Baste señalar, para nuestros propósitos, que el filósofo alemán quería subrayar cómo el manto de la verdad ejerce una fuerza

monopolística. Verdad implica correcto, mejor y bueno. Cualquier cosa que sea aprobada como verdad actúa entonces para devaluar otros dominios de creación y experiencia, como el arte y el mito, que se encuentran fuera de la órbita de la "verdad" y, en consecuencia, asignados a la categoría de "falsedad". En este campo ideológico binario, el arte se convierte en un ciudadano de segunda clase en la vida pública de las ideas, mientras que a la fantasía y al mito apenas si se les permite unirse a la fiesta.

Nietzsche estaba en sintonía con la vitalidad de la sensualidad, el mito y el arte. Música, poesía e incluso la risa demencial del embaucador Dionisio, a quien defendía, ofrecen una vida estética de placer.[212] Son búsquedas a través de las cuales el ser humano es capaz de superar sus límites y la condición trágica de la vida: «No con la cólera, sino con la risa se mata. ¡Adelante, matemos el espíritu de la seriedad!»[213]

Más que cualquier otro movimiento político en tiempos recientes, Anonymous, y especialmente su vástago LulzSec, proporcionan una poderosa conformación social a varias de estas cuestiones filosóficas planteadas por Nietzsche. Si Nietzsche sostenía que no hay nada sagrado y abogaba por una vida de encantamiento, entonces LulzSec y Anonymous hicieron realidad estas máximas. Ellos se atrevieron a subvertir y a vulnerar la ley, la etiqueta y las costumbres formales, y experimentaron con el arte de la transgresión. Y nos recordaron: para convertir la vida en arte, y el arte en vida, a veces es necesario transgredir.

Y transgredir es una tarea difícil. Hace tiempo, cuando impartía un curso de comunicación y cultura en la universidad, solía pedirles a mis alumnos que infringieran una norma en público y luego volviesen para hablar de su experiencia. Con la única excepción de uno o dos excéntricos, que disfrutaron con la tarea asignada (una de ellas nos contó alegremente que su madre la había sacado de paseo llevando un collar y una correa, como si fuese un perro, por las calles de Nueva York, y que prácticamente nadie se inmutó), para todos ellos fue un ejercicio extraordinariamente duro, incluso doloroso. De hecho, prácticamente la cuarta parte de la clase se saltó las reglas de un modo que difícilmente podría calificarse de muestra de "audacia", como pedirle a un desconocido si podía compartir su mesa en un café.

La presión para que nos ajustemos a las convenciones y aceptemos la sabiduría convencional es enorme, y a menudo por buenas razones. Gran

parte del corpus teórico de Nietzsche pone al descubierto esta tendencia y advierte acerca de sus efectos perniciosos, que es precisamente lo que abordan los mitos del embaucador, una y otra vez, si bien de una forma diferente. En efecto, uno de los personajes más famosos de Nietzsche, Zaratustra, es una figura similar a un embaucador. Después de haber vivido como un ermitaño durante una década en las montañas, descubre que se pueden superar las convenciones sociales en favor de deseos e ideas autodefinidos. Desciende entonces de la montaña para compartir esta visión, promoviendo un proceso al que llama "autosuperación". Anonymous y LulzSec han existido como instanciaciones de Zaratustra. LulzSec fue un paso más allá que Anonymous, vulnerando incluso las reglas que habían arraigado de forma inadvertida en el propio Anonymous, planteando un desafío a este orden emergente.

Es raro que algo que realmente se parece al mito del embaucador aparezca en medio de nuestra realidad contemporánea, y mucho más con tanto entusiasmo y presencia pública. Estos hackers, en su sacrificio (y el sacrificio de otros) cumplieron con la función de recordarles a muchos la necesidad, el placer y el peligro de la subversión.

La admiración que muchos sentían hacia Anonymous y LulzSec puede ser aclarada por la visión de Walter Benjamin con respecto al gran criminal que, «sin importar lo repelentes que puedan haber sido sus fines, ha despertado la admiración secreta del público».[214] Esta admiración se deriva del hecho de que la criminalidad pone al descubierto los límites del monopolio que ejerce el Estado sobre la violencia y la fuerza de la ley. Pero LulzSec y Anonymous excedían fundamentalmente el marco de la criminalidad, aun cuando eran incapaces de escapar completamente a su órbita. LulzSec y Anonymous, a diferencia de las organizaciones criminales, no actuaban por el lucro personal y, en el caso de Anonymous, ha existido una notable presión social para acallar el interés propio, la fama personal y el reconocimiento. Anonymous interpretó la lección más amplia y nietzscheana encarnada en Zaratustra: representar el deseo secreto de quitarse —al menos por un momento—los grilletes de la normatividad y alcanzar la grandeza, la voluntad de poder puesta al servicio de metas colectivas y altruistas en lugar de los deseos individualistas y que buscan el interés personal. El caos artístico de Anonymous y LulzSec, parafraseando a Nietzsche, dio a luz a una estrella danzarina. Si parezco manifiestamente

romántica con respecto a LulzSec y a esta era de Anonymous, es posible que lo sea. Pero los acontecimientos ulteriores aseguraron que esta fase de luna de miel era efímera. Ahora podemos centrarnos en la muerte de LulzSec y en la aparición de AntiSec y comprobar cómo este mito impresionante fracasó cuando Anonymous se vio parcialmente eclipsado por el culto a la personalidad.

Capítulo 9

AntiSec

Un día de febrero de 2011, un hacker de Chicago de 26 años se conectó al servidor de IRC de AnonOps y se dijo, «Bien, aquí tenemos una conversación productiva». Anonymous se encontraba en pleno proyecto de atacar a los tristemente famosos hermanos Koch, los principales contribuyentes del gobernador republicano de Wisconsin, Scott Walker. Aquel gélido invierno, activistas de todo el Estado habían marchado desde las granjas y las fábricas hacia el capitolio del Estado para protestar contra el gobernador Walker, que estaba impulsando una ley que privaría a los empleados del Estado de su derecho a la negociación colectiva. Este hacker observó cómo Anonymous lanzaba un ataque DDoS contra Americans for Prosperity, un grupo defensor del mercado libre financiado por los hermanos Koch.

En Chicago también hacía un frío glacial. El inclemente viento invernal que se arremolinaba en las esquinas y aullaba por los callejones había tomado la ciudad. Este hacker, Jeremy Hammond, llevaba conectado apenas veinte minutos cuando perdió la conexión a Internet. Con un suspiro de frustración, levantó su cuerpo delgado de metro ochenta de la silla y salió de casa. Permaneció junto a la puerta trasera, con los dedos entumecidos por el intenso frío, mientras intentaba desesperadamente ajustar la antena del Wi-Fi. Su portátil estaba conectado a la antena, activando “aircrack-ng” (una suite de software de seguridad inalámbrica) y hacía todo lo posible por penetrar en la red inalámbrica del vecino. Hammond permaneció inmóvil. Sabía que hasta el más leve movimiento podía afectar la señal inalámbrica. Eran las tres de la madrugada y se estaba congelando. Entrar en la casa no sería de mucha ayuda; hacía meses que no

funcionaba la calefacción. Con la conexión a Internet finalmente restablecida volvió a conectarse al canal de IRC y permaneció durante horas bañado por la luz azulada que proyectaba la pantalla de su portátil.

Mientras Hammond leía todo lo que podía acerca de las últimas incursiones activistas realizadas por Anonymous, sintió un pinchazo en el alma. Se identificaba con Anonymous y quería formar parte de ese colectivo. Hammond era un apasionado activista político; era —y sigue siendo—, sin duda, uno de los hacktivistas estadounidenses más prolíficos, inflexibles y decididos que hayan puesto los dedos sobre un teclado. Con poco más de veinte años, la acción directa ya formaba parte de su estilo de vida; entre los 18 y los 28 años fue arrestado en ocho ocasiones mientras participaba en protestas políticas. En la Convención Nacional Republicana de 2004, celebrada en Nueva York, fue detenido durante una protesta con cacerolas; al año siguiente se movilizó contra un grupo neonazi en Toledo, Ohio, y fue arrestado por violar una orden que prohibía las manifestaciones callejeras. En fechas más recientes, en 2010, después de quemar una bandera olímpica como protesta por la candidatura presentada por Chicago para organizar los Juegos Olímpicos de 2016, fue condenado a dieciocho meses de libertad condicional y 130 horas de servicio comunitario. Hammond se define orgullosamente como anarquista porque cree apasionadamente en los «colectivos sin liderazgo basados en la libre asociación, el consenso, la ayuda mutua, la autosuficiencia y la armonía con el medioambiente».[215]

En el verano de 2011, con la nieve ya lejana en el recuerdo, Hammond estaba comprometiendo activamente servidores y sitios web con propósitos políticos. Esta actividad resultó fatídica para él, ya que poco más de un año después sería arrestado y tendría que cumplir una condena a diez años en una prisión federal. Hammond me habló sobre su hacktivismo pasado y su implicación con Anonymous en septiembre de 2013, durante nuestro primer y único encuentro cara a cara en el Metropolitan Correctional Center de Nueva York, donde permanecía encerrado a la espera de su sentencia. Después de su arresto en marzo de 2012 nos habíamos comunicado a través de los anticuados sobres de papel con sellos (Hammond colocaba sus sellos al revés). Cuando le conocí llevaba puesto un mono marrón enorme encima de un cuerpo que ya no tenía el aspecto desgarbado de su pasado como programador. Sus abultados antebrazos —el indicio más visible de los casi

treinta kilos de musculatura que había ganado en prisión— descansaban sobre la mesa marrón de la inhóspita sala de reunión de los presos. La banda sonora la proporcionaban el zumbido y el chasquido de las luces fluorescentes, cuyos destellos rebotaban contra los bloques de hormigón blancos. Después de haber eliminado toda calidez estética de la sala, los administradores de la prisión encontraron una manera de empeorarla aún más, volviéndola helada.

En este ambiente encantador, mientras Hammond se prodigaba en detalles sobre su pasado, resultó cada vez más evidente que sus habilidades técnicas habían sido perfeccionadas específicamente por sus capacidades políticas.

Habiéndose criado con su hermano gemelo y su padre en los alrededores de Chicago, empezó a entretenerse con sus juegos de ordenador apenas abandonada la cuna. A los diez años se graduó programando sus propios juegos en QBasic en un portátil en blanco y negro de 10MHz con MS-DOS6 y Windows 3.1. Poco después se conectó a la red y creó un canal de IRC para desarrollar juegos. También descubrió y devoró géneros literarios relacionados con los hackers, como *textfiles* (conocidos también como *philes*) y *zines* (publicaciones pequeñas, no comerciales y de poca difusión). Habitualmente estos textos, «que enseñan las técnicas y el credo del underground», como señala Bruce Sterling, «son valiosas reservas de conocimiento prohibido».[216]

La mayoría de ellos muestra un fuerte antiautoritarismo o sugerencias inquietantes, características que son notablemente evidentes en sus títulos:

Hacking Bank America BANKAMER.ZIP
Chilton Hacking CHHACK.ZIP
Hackers Digest DIGEST.ZIP
Phortune 500 Guide to Unix P500UNIX.ZIP
Radio Hacking REDHACK.ZIP
Anarchist Book ANARCHST.ZIP
Barbiturate Formula BARBITVA.ZIP
Electronic Terror ELECTERR.ZIP
Briefcase Locks MRSHIN.ZIP
More Pranks to Pull on Idiots! PRANK.TXT[217]

Hammond engulló este material y supuso (erróneamente) que la mayoría de

los otros hackers compartía sus sensibilidades políticas. No fue hasta que comenzó el instituto, cuando empezó a asistir a las reuniones locales de la revista *2600*, que experimentó una especie de brusco despertar. Recuerda que la mayoría de los participantes eran “súper sombreros blancos” cuya visión política distaba mucho de sus incipientes sensibilidades anticapitalistas. Pero, debido a que también se identificaba como hacker, disfrutaba asistiendo a esas reuniones. Veía la utilidad de aprender de esas personas.

Y entonces, según me explicó, el proceso de politización personal se intensificó un poco más tarde, cuando «Bush robó las elecciones, se produjo el 11/9 y se aprobó la Ley Patriótica». A los veinte años cofundó el sitio web radical llamado *Hack This Site* con una *zine* llamada *Hack This Zine*. Estos títulos se inspiran en *Steal This Book*, el manual-manifiesto contracultural de los años sesenta escrito por Abbie Hoffman. (Los yippies, integrantes de la Línea del Partido Internacional de la Juventud, publicaron el primer *zine* hacker/phreak, *The Youth International Party Line*, que abogaba por estafar a AT&T, alias “Ma Bell”, como un acto revolucionario. La publicación posterior, *Technical Assistance Program* (TAP), exhibiría una retórica política abiertamente izquierdista.) *Hack This Site* incluía cuestiones relativas a la seguridad informática, pero también profundizaba en los acontecimientos y tendencias políticas radicales repartidos por todo el mundo, como el movimiento contra la guerra en Afganistán y las amenazas potenciales a la democracia que representaban las máquinas de votación informatizadas.

Aunque Hammond fuese una anomalía en el panorama hacker estadounidense, en el mundo había suficientes almas gemelas para constituir una banda pequeña, pero combativa, de guerreros tecnológicos radicales. Su *zine* ayudó a generar una cohorte de hackers con tendencias izquierdistas. De hecho, uno de los hackers de LulzSec con vocación más política, Donncha O’Cearbhaill, alias Palladium, había sido lector antes de que Hammond y él se conocieran en línea. Y cuando Hammond no escribía para su *zine*, canalizaba sus habilidades técnicas más directamente hacia sus objetivos políticos.

En el curso de uno de sus primeros hackeos, antes de comenzar a participar en Anonymous —de hecho, antes incluso de que Anonymous existiera como un nombre para canalizar las causas relacionadas con el

activismo— Hammond dejó la imagen de Guy Fawkes en un sitio web desfigurado. Cuando se refirió brevemente a su desfiguración con Guy Fawkes y describió su pasión por la película *V de Vendetta*, sus ojos azules se iluminaron, su pálido rostro cobró vida y la austera habitación en la que nos encontrábamos pareció más acogedora. Le insistí para que me diese más detalles.

En marzo de 2006, solo un año después de que iniciara sus hackeos de naturaleza política, ya había constituido un equipo con The BrigadaElektronica, una asociación informal de hackers radicales anónimos. Esta coalición hackeó los sitios web de la Policía Nacional de Filipinas, el Palacio de Malacañang (la residencia oficial del presidente filipino), la Oficina del Presidente de Filipinas y el Colegio Nacional de Defensa de Filipinas, en una muestra de solidaridad con el grupo Sagada 11. Este grupo de activistas incluía a unos cuantos que trabajaban voluntariamente con Food Not Bombs, que habían sido detenidos en la provincia septentrional de Luzón y se enfrentaban a cargos de terrorismo.[218] (Food Not Bombs es una asociación de colectivos radicales que sirven comida vegana y vegetariana a personas que padecen hambre.)

Hammond no era el único anarquista en ciernes aficionado al éxito de taquilla de Hollywood *V de Vendetta*, estrenada el mismo mes en que llevó a cabo su hackeo en apoyo a Sagada 11. El antihéroe de la película lleva una máscara de Guy Fawkes. Fawkes fue una figura conocida principalmente como una especie de mascota del regicidio británico del siglo XVII. Sus fallidos intentos de regicidio se conmemoran hasta el día de hoy en forma de un festejo británico que lleva su nombre y que celebra la continuidad de la monarquía con grandes hogueras. El escritor británico Alan Moore recuperó esta figura mitificada para crear un cómic distópico, que se convirtió en una película de Hollywood y provocó la reinvención del rostro de Fawkes como el del terrorista-convertido-en-icono-de-la-resistencia por excelencia. Si bien todos los símbolos están abiertos a la interpretación, algunos son más flexibles que otros. Mientras que el símbolo de la paz representa una sola postura, este hombre silencioso y sonriente ha acumulado a lo largo de los años múltiples significados antes de convertirse en el rostro de la disidencia popular.

Poco después de sus incursiones en el hackeo político, Hammond fue arrestado y encerrado en una prisión federal entre 2006 y 2008. Se había

infiltrado digitalmente en una organización de derechas llamada "Protest Warrior", cuyo lema es «Combatiendo a la izquierda... y haciéndolo correctamente» (jugando con el doble sentido de la palabra *right*, que significa "correctamente" y también "derecha") y sustrajo información de tarjetas de crédito de la base de datos del sitio web de la organización. Puesto que nunca utilizó la información de las tarjetas, tan solo se le acusó de intrusión informática, con lo que se libró de una condena más dura y de las multas que a menudo acompañan el uso fraudulento de tarjetas de crédito (el fiscal pedía una condena de cinco años de prisión, además de 2,5 millones de dólares de multa, argumentando que «Mientras que Jeremy Hammond intentó que fuese una acción política, nosotros queríamos que la pena fuera por lo realmente ocurrido, el robo de tarjetas de crédito»).[219] Hammond, condenado a veinticuatro meses de cárcel y a pagar una multa de 5.358 dólares, fue enviado a una prisión de seguridad media y cumplió dieciocho meses de su condena.

Durante nuestra entrevista me hizo una confesión sorprendente. En 2008, cuando Anonymous comenzó a adoptar la máscara de Guy Fawkes que él tanto adoraba, al principio fue rechazado por el grupo. Entonces descartó a Anonymous, tachándolos de *script kiddies* ("programadores novatos") y consideró que la cultura del "todo vale" característica del troleo descarriado —que a veces cruzaba la línea roja del racismo— resultaba "alienante". Pero éstas no eran razones de peso comparadas con su amplio rechazo del hacktivismo en general. Después de algunos años dedicado al hackeo político, y de dos años en prisión debido a esas actividades, se preguntó si «como ecologista [...] estaba apoyando a la bestia industrial a través de la tecnología». Durante algún tiempo la respuesta fue «sí» y dejó de hacerlo.

Pero con la aparición de WikiLeaks, y con las filtraciones aportadas sobre todo por Chelsea Manning, vio el potencial que tenía la tecnología «de desenmascarar delitos». Durante la lectura de su sentencia, después de su temporada de hackeos para Anonymous, rendiría tributo a Manning: «Asumió un enorme riesgo personal al filtrar esta información, en el convencimiento de que la opinión pública tenía derecho a conocerla y esperando que sus revelaciones fuesen un paso positivo para acabar con estos abusos. Resulta desolador saber el trato cruel que recibe en su confinamiento militar.»

Hammond hizo las paces con Anonymous a principios de 2011. Se unió a AnonOps durante la OpWisconsin, pero permaneció en gran medida como espectador. Mientras aprendía los gajes del oficio también empezó a relacionarse con otros hackers. El 21 de junio de 2011, Hammond decidió finalmente dar el salto. Primero se intentó acercar a Sabu y quiso entregarle material pero, después de fracasar en su intento, envió un mensaje privado a dos miembros de LulzSec, primero a Topiary y luego a tflow, ofreciéndose a descargar algunos “caramelitos” que tenía en su poder. Hammond había conseguido recientemente acceso privilegiado al sitio web del Departamento de Seguridad Pública de Arizona y había desviado los datos que encontró allí. LulzSec aceptó finalmente la custodia de esa información y la hizo pública en cuatro tandas bajo el título de “Chinga La Migra” (expresión en español para “Que se joda la Policía de Inmigración”). La información incluía mensajes de correo electrónico, nombres, números de teléfono, direcciones de domicilios particulares y contraseñas pertenecientes a funcionarios de Arizona, junto a material operativo como boletines de inteligencia privados y manuales de formación.

El momento era perfecto. Cuando Hammond entregó los datos, LulzSec se encontraba en medio de una transformación radical, de fabuladores-embaucadores de Internet a militantes revolucionarios. Tenían una nueva agenda y una nueva bandera: “AntiSec”, abreviatura de Anti-Security. Este cambio es difícil de explicar. Los participantes confirmaron que incluso para ellos este período se envolvía en el caos. Un Anon me confesó durante una entrevista: «Era caótico en cuanto a la gran cantidad de subgrupos que se formaban, fragmentaban y redefinían a sí mismos... Era la época de LulzSec, AntiSec, TeaMp0isiN, el A-Team, CabinCr3w, Buccaneers, Panther Moderns, etcétera.» Misterios aparte, una cosa estaba clara: durante el verano de 2011, Anonymous había experimentado una explosión volcánica de equipos de hackers. Mientras que anteriormente una única red de IRC (AnonOps) y un grupo secesionista (LulzSec) dominaban el panorama estadounidense y europeo; ahora había un archipiélago de islas de hackers —con AntiSec como la más visible y célebre del grupo— que emergía súbitamente de las aguas de Anonymous.

«Es ahora o nunca. Subid a bordo, os estamos esperando»

A comienzos de junio de 2011, LulzSec navegaba viento en popa dejando una estela extravagante para disfrute de otros internautas. En aquel momento no lo sabían, pero navegaban directamente hacia la tormenta. De una forma aparentemente inesperada, el 19 de junio de 2011, cuatro días antes del lanzamiento de Chinga La Migra, LulzSec desplegó la "Operación AntiSec". Esta operación se anunció, como era habitual, mediante un comunicado de prensa publicado en Pastebin.com. Pero el comunicado contenía una diferencia fundamental: su lenguaje. Con solo algún toque de humor (alguna referencia a la sangre del lagarto y a la canción de la serie *Vacaciones en el mar*), el tono era sorprendentemente revolucionario. El comunicado también expresaba algo que LulzSec nunca había reivindicado antes: que la operación era un proyecto de Anonymous,

> Bienvenidos a la Operación Anti-Security (#AntiSec). Animamos a cualquier embarcación, grande o pequeña, a abrir fuego contra cualquier gobierno o agencia que se cruce en su camino. Apoyamos plenamente la ostentación de la palabra "AntiSec" en cualquier desfiguración de un sitio web del gobierno o en forma de graffiti físico.
>
> Ya sea que estéis navegando con nosotros o contra nosotros, que guardéis rencores del pasado o un ardiente deseo de hundir nuestro buque solitario, os invitamos a uniros a la rebelión. Juntos podemos defendernos para que nuestra privacidad no sea invadida por abusones especuladores. Vuestro sombrero puede ser blanco, gris o negro, vuestra piel y raza no importan. Si sois conscientes de la corrupción, exponedla ahora, en nombre de Anti-Security.
>
> La máxima prioridad es robar y filtrar cualquier información clasificada del gobierno, incluidos colas de impresión de correos electrónicos y documentación. Los objetivos principales son los bancos y otras instituciones de alto nivel. Si ellos intentan censurar nuestros avances, nosotros destruiremos al censor con cañonazos ungidos con sangre de lagarto.
>
> Es ahora o nunca. Subid a bordo, os estamos esperando.[220]

¿Por qué Topiary, que redactó el comunicado, impulsó esta postura revolucionaria? Todas las pruebas señalan a Sabu. Pocas semanas antes de la publicación del comunicado de prensa, Sabu había reivindicado online la reactivación de un viejo proyecto de AntiSec.

El movimiento antiseguridad había prosperado brevemente a finales de siglo entre algunos hackers de sombrero negro que despreciaban a la industria de seguridad en general y a los hackers de sombrero blanco en particular. Fue un período en el que los hackers buscaban y encontraban empleo cada vez más a menudo en la industria de seguridad. Bajo la capa manto de la antiseguridad, un grupo de hackers de sombrero negro colocó en el punto de mira a profesionales de la seguridad —doxeándolos y robando sus correos electrónicos— para protestar por la práctica cada vez más frecuente de revelar públicamente los exploits y vulnerabilidades. Su razonamiento, ofrecido a modo de documento fundacional, era el siguiente:

> La finalidad de este movimiento es fomentar una nueva política de anti revelación entre las comunidades de seguridad informática y en red. El objetivo básico es no desanimar la publicación de todos los avances y noticias relacionados con la seguridad, sino frenar la revelación de todos los exploits y vulnerabilidades desconocidos o no públicos. En definitiva, esto acabaría con la publicación de los materiales privados que podrían permitir que los *script kiddies* comprometieran los sistemas a través de métodos desconocidos.[221]

Si bien esta declaración puede sonar razonable, las acciones llevadas a cabo por el grupo eran agresivamente audaces. Un reciente manifiesto antiseguridad refleja el caos que estos hackers provocaron en la industria de seguridad (*véase* la figura de la página siguiente). Aunque pueda parecer extraño, parte de la motivación que hay detrás de la antiseguridad original era la preservación cultural, «recuperar el escenario».

La visión original de la antiseguridad era un animal diferente del que habían concebido Sabu y Anonymous. Mientras que el movimiento contemporáneo AntiSec mostraba escaso respeto por los sombreros blancos y estaba asqueado por lo que consideraba como una muestra flagrante de avaricia en la industria de seguridad, estos no eran sus principales enemigos.

Antisec

/Expuesto

- **Que se joda la divulgación total.**
- **Que se joda la industria de seguridad.**
- **Mantener privados los días cero.**
- **Hackear a todos los que puedas y luego hackear a algunos más.**

Mezclarse.
Ganarse la confianza.
No confiar en nadie.
Poseer a todos.
No revelar nada.
Destruir todo.
Recuperar el escenario.
No venderse nunca, no rendirse nunca.
Entrar como anonymous, Marcharse sin dejar rastro.

[Buenas lecturas:
Grupo Antisec Expuesto [espejo] [espejo] [espejo] [espejo] [espejo]

[Archivos adjuntos:
Archivos adjuntos del Grupo Antisec [espejo] [espejo] [espejo] [espejo] [espejo]

[Lista de verificación / Objetivos:
Eliminar todo foro público, grupo o sitio web que ayude a promover exploits y herramientas o tengan secciones de exhibición. Publicar los exploits equipados con /bin/rm a los sombreros blancos, dejar que rm sus propias boxes para ti.
Difundir el movimiento antiseguridad.
Revivir pr0j3ct m4yh3m.

[Reglas de Compromiso:
No volverse demasiado prepotente.
No subestimar a nadie.

[Contacto / Presentar documento:

En cambio, la reactivación de AntiSec estaba motivada por un sentido más general de la justicia. El objetivo era penetrar en bancos, gobiernos, empresas de seguridad y otra corporaciones en busca de información políticamente condenatoria y susceptible de ser filtrada. Y tal vez lo más importante de todo, la manifestación contemporánea de la antiseguridad no trabajó de modo silencioso.

La primera mención pública que hizo LulzSec de AntiSec fue en Twitter: «Reuníos, éste es un nuevo cibermundo y lo estamos iniciando juntos. Habrá objetivos más grandes, habrá más enrutamientos. #ANTISEC.»[222]

Solo tres días antes de que colgaran este mensaje, el 7 de junio de 2011, a las 22.15 horas, el FBI visitó un imponente complejo de viviendas llamado Jacob Riis Houses, en el Lower East Side de Manhattan. Los agentes federales acudieron a este bastión puertorriqueño para arrestar a Héctor Monsegur, alias *Sabu*. Según una orden de registro filtrada que el FBI presentó para acceder a la cuenta de Facebook de Monsegur, una corporación hackeada previamente por Anonymous sacrificó una dirección de IP que entregó a las fuerzas de la ley. El FBI recuperó la información del suscriptor de la dirección de IP, lo que condujo a las direcciones postal y de correo electrónico de Monsegur. Las autoridades buscaron acceder a la cuenta de Facebook de Monsegur porque las «fotografías» les permitirían «confirmar la identidad del individuo que colaboró en la intrusión no autorizada» y posiblemente también obtener pistas si Monsegur había compartido cualquier información en la plataforma de las redes sociales con sus colegas hackers. Aunque solo tenía 27 años, era padre adoptivo de las dos hijas de su tía, que cumplía una pena de cárcel, que en aquella época tenían menos de 8 años. Además de su actividad en Anonymous/LulzSec, el FBI tenía pruebas que lo relacionaban con un fraude cometido con tarjetas de crédito. Ante la perspectiva de pasarse décadas entre rejas y de perder a sus dos hijas adoptivas, Monsegur cambió de bando.

Apenas cuatro días antes del arresto de Sabu, el equipo de LulzSec estaba preocupado por la posibilidad de que algunos de sus afiliados

hubiesen abandonado el barco. Sabu había afirmado que iba a borrarlo todo:

<Neuron>: Sabu, ¿hemos perdido gente?
<storm>: de acuerdo
<storm>: ¿es así?
<Sabu>: sí
<storm>: ¿quién?
<Sabu>: recursion y devurandom se han retirado respetuosamente
<Sabu>: diciendo que no están preparados para eso
<Neuron>: yo ya estoy borrando todo mi escritorio
[...]
<Sabu>: sí
<Sabu>: borra todo
<Sabu>: yo estoy limpiando toda mi mierda ahora

Cualquier cosa que hubiera hecho o no en aquel momento, Sabu pasó de ser un hacktivista radical a instalarse en el bolsillo del FBI, donde facilitó un portal directo a LulzSec. Al equipo de LulzSec, constantemente conectado, le pareció sospechosa la ausencia de Sabu durante veinticuatro horas. Para hacer una comprobación cuando volvió a conectarse, le pidieron que enrutara un servidor, cosa que hizo y que sirvió para disipar cualquier preocupación. El FBI, por supuesto, le dio su bendición para que procediera y pudiera mantener así su tapadera.

Poco después de su arresto, Sabu subió el tono de la retórica de AntiSec previamente insinuada en un breve mensaje de Twitter. Debía de saber que Hammond lo encontraría apetecible. Es probable que Hammond estuviese dentro del radar del FBI, puesto que era uno de los pocos anarquistas y hackers en los Estados Unidos que ya había pasado algún tiempo en prisión. El cambio retórico marcado por AntiSec podría haber sido fácilmente la continuación de un compromiso sincero. Es posible que nuca lo sepamos. Pero lo que sí sabemos es que Sabu, poco después de haber cambiado de bando, presionó para que el comunicado de prensa de AntiSec incluyera un lenguaje políticamente cargado y que Topiary redactó voluntariamente. Topiary me explicó vía correo electrónico que

> Sabu estaba muy interesado en que redactara este mensaje, pero tal vez estaba más obsesionado con la cuenta en twitter de un seguidor de

> LulzSec en aquella época y lo veía como una plataforma desde la cual impulsar esta clase de postura política. En aquel momento no parecía más que una actuación adolescente equivocada y angustiada, pero por supuesto para lo demás fue tomado de un modo mucho más serio.

El público, los periodistas y el propio Anonymous ignoraban que el FBI tenía a Sabu perfectamente controlado, pero todos se dieron cuenta del tono tan distinto del comunicado de prensa respecto del estilo habitual de LulzSec. Los medios de comunicación, desde AdBusters hasta Fox News, informaron sobre el comunicado, y una media docena de periodistas lo analizaron para tratar de entender lo que estaba ocurriendo. Stephen Chapman, de ZDNet, planteó la pregunta clave:

> Lo que hasta este momento ha existido como un propósito vago consistente en una serie de objetivos aleatorios e insustanciales, se está configurando ahora como un movimiento antigubernamental/antiestablishment plenamente desarrollado y de proporciones potencialmente épicas. ¿Ha comenzado finalmente la revolución digital, algo que llevamos años viendo a Hollywood escenificar? Quizás.[223]

Todo el mundo se preguntaba, incluso yo, si se trataba de otra broma o de la expresión de un sentimiento auténtico.

Al día siguiente llegó la respuesta de LulzSec. Cumplieron la promesa de la Operación AntiSec utilizando la botnet de Ryan Cleary para lanzar un ataque DDoS contra la Agencia contra el Crimen Organizado de Gran Bretaña. Al día siguiente, 21 de junio, las autoridades policiales arrestaron a Cleary en su residencia de Essex, a las afueras de Londres. Los periódicos ingleses salieron con docenas de imágenes del joven en cuestión, uno de los principales hackers de AnonOps y afiliado de LulzSec. Según su retrato en las noticias, Cleary se ajustaba al estereotipo de joven solitario y disfuncional. Regordete y con la piel de color blanco lechoso, Cleary raramente abandonaba su habitación que, aunque no estaba técnicamente en un sótano, sin duda lo parecía, puesto que tenía la ventana permanentemente tapada con papel de aluminio. Los tabloides británicos no perdieron ni un segundo en dar un cariz sensacionalista a todos y cada uno

de los detalles.

Fue justamente en medio de este ambiente frenético que Hammond decidió ponerse en contacto con LulzSec con su material sobre Arizona. Su intención original había sido entregarle ese material a Sabu, pero Sabu se mostró súbita y extrañamente insensible a sus consultas. Almas aparentemente gemelas, Hammond y Sabu habían establecido un vínculo en torno al objetivo compartido de unir a los diferentes sombreros negros para protestar contra la injusticia y la opresión.

De modo que Hammond, que operaba bajo el nombre de “Anarchaos”, envió mensajes privados a Topiary y tflow, subrayando que no quería «tocar el servidor de inicialización de torrent ni con un palo de dos metros». Tflow aceptó alegremente los “caramelitos” y LulzSec colgó inmediatamente el material, incluyéndolo en los servidores de torrent de Pirate Bay el 23 de junio. Como Hammond no se había ganado la confianza del núcleo principal de hackers de LulzSec, no se le permitió acceder a sus salas privadas. Pero su hackeo proporcionó el catalizador que permitió hacer realidad la visión de AntiSec. Hammond redactó personalmente el comunicado de prensa de Chinga La Migra:

> Estamos destapando cientos de boletines de inteligencia privados, manuales de formación, correos electrónicos personales, nombres, números telefónicos, direcciones y contraseñas pertenecientes a las fuerzas de la ley en Arizona. Nuestro objetivo específico es el AZDPS (Departamento de Seguridad Pública de Arizona) porque nos oponemos al SB1070 y al estado policial antiinmigración de perfil racista que es Arizona.
>
> Los documentos clasificados como “sensibles para los cuerpos y fuerzas de seguridad”, “no para distribución pública”, y “solo para uso oficial” están relacionados principalmente con la patrulla de fronteras y las operaciones de contraterrorismo, y describen el empleo de informantes para infiltrarse en numerosos cárteles, bandas, clubes de motoristas, grupos nazis y movimientos de protesta.
>
> [...]

> Los hackers de todo el mundo se están uniendo y adoptando acciones directas contra nuestros opresores comunes: el gobierno, las corporaciones, la policía y los militares mundiales. ¡Nos volveremos a ver muy pronto! ;D[224]

Poco después de la divulgación de Chinga La Migra, Hammond, aún en libertad condicional debido a su hackeo anterior, recibió una visita de la policía de Chicago y el FBI para hacer una verificación de su libertad condicional. A Hammond le resultó extraño que un agente del FBI acompañase al funcionario de libertad vigilada para hacer una comprobación de rutina. «Cuando descubrieron la K2 [marihuana sintética], presentaron cargos estatales contra mí de delito grave por posesión de marihuana, cargos que quedaron en nada cuando volvieron los resultados de la droga», explicó Hammond. Su estancia de varias semanas en la cárcel impidió que Hammond pudiera presenciar la controversia que la revelación de los documentos de Arizona había provocado entre los miembros de LulzSec. Varios de ellos, como tflow, pwnsauce y más tarde Topiary, lamentaron su decisión de hacer públicos esos datos.

Aunque estos jóvenes habían doxeado anteriormente un lote completo de ejecutivos corporativos y divulgado otros datos igualmente sensibles, poner a oficiales de policía en el punto de mira era una acción que implicaba un riesgo mucho mayor. Este territorio, aunque familiar para Hammond, era desconocido para ellos.

De hecho, tflow, que entonces tenía 16 años, animó al grupo a disolver LulzSec. Solo había estado activo cincuenta días, pero ese es el ciclo vital en Internet. Sorprendentemente, todos ellos, incluido Sabu, estuvieron de acuerdo al principio. Pero luego, sin previo aviso, Sabu cambió de opinión. Tflow me lo explicó: «Como consecuencia de este asunto, él estaba simplemente cabreado porque todos queríamos largarnos a pesar de que él no quería que lo hiciéramos, y casi siempre consigue lo que quiere a través de la manipulación.» Ryan Ackroyd (alias Kayla) también recordó una de las tácticas más manipuladoras —y profundamente irónicas— practicadas por Sabu: «Le recuerdo diciendo (no palabra por palabra) algo acerca de poner en riesgo a los chicos habiendo llegado tan lejos y esas cosas y que era injusto rendirse.»

A pesar de las exhortaciones de Sabu, finalmente prevaleció el bando

de tflow. LulzSec se retiró a finales de junio de 2011. Ellos, naturalmente, no pudieron evitar marcharse con estilo y, por tanto, el 25 de junio llevaron a cabo una mega divulgación, incluido el texto de un manual de trabajo en red interno de AOL, medio gigabyte de datos internos de AT&T y los correos electrónicos, nombres de usuario y contraseñas de usuario encriptadas para sitios que iban desde HackForums.net hasta la librería en línea de la OTAN. Más interesante incluso que los propios datos divulgados —el menos desde la perspectiva del engaño y la construcción de mitos—fue la declaración final de LulzSec, redactada nuevamente por Topiary:

> Durante los últimos cincuenta días hemos estado perturbando y exponiendo a corporaciones, gobiernos, a menudo a la población en general, y muy posiblemente todo lo que hay en medio, solo porque podíamos hacerlo. Todo para entretener egoístamente a los demás; vanidad, fama, reconocimiento, todas esas cosas quedan ensombrecidas por nuestro deseo de aquello que todos amamos. La emoción pura, ininterrumpida, caótica del entretenimiento y la anarquía. Es lo que todos anhelamos, incluso los políticos aparentemente inertes y los autoproclamados fracasados gélidos de mediana edad.[225]

El comunicado de prensa le pasaba el testigo de LulzSec al incipiente movimiento AntiSec. Estos hackers querían, en palabras de tflow, «que el legado de hackeos de LulzSec continuase». La declaración final concluye:

> tras de la máscara, tras la locura y el caos, creemos realmente en el movimiento AntiSec. Creemos en él tan firmemente que lo hemos recuperado, para disgusto de aquellos que buscan un lulz más anárquico. Esperamos, deseamos, hasta imploramos, que el movimiento se manifieste en forma de una revolución que pueda continuar sin nosotros... Por favor, no os detengáis. Juntos, unidos, podemos pisotear a nuestros opresores comunes e imbuirnos del poder y la libertad que merecemos.

En prisión, Hammond contaba los días que le faltaban para poder regresar a su recién descubierta comunidad de hackers súper politizados. Una vez en

libertad estaba «preparado para volver a lucha», según me confesó. No tuvo ningún problema en encontrar a camaradas dispuestos.

No obstante, el éxito futuro de AntiSec fue incierto hasta que convergieron tres factores. El primero, que Sabu, que ahora trabajaba a tiempo completo como informante, convirtió en su misión personal mantener AntiSec a flote. El segundo, que Hammond actuó como el confederado perfecto. Hacker talentoso que creía en la misión de AntiSec, se convirtió en su infatigable caballo de batalla, dedicando finalmente la mayor parte de su tiempo libre a este proyecto. El tercer factor fundamental fue la existencia de un equipo más amplio. A pesar de que algunos miembros de LulzSec habían dicho adiós definitivamente, varios de ellos se incorporaron al nuevo equipo. El equipo de AntiSec constituido lo formaron entre ocho y doce participantes principales, más de los que había tenido nunca LulzSec. Compuesto por hackers y un puñado de estrategas, el equipo se instaló en un canal secreto (con el nombre no tan secreto de "#antisec") en un servidor llamado "cryto". Muchos de ellos habían colaborado anteriormente durante las operaciones de las primaveras árabe y africana. Yo misma conocí a varios de ellos de aquella etapa, cuando frecuentaba #freedommods, uno de los canales sociales solo por invitación para las operaciones revolucionarias.

Sabu, tantas veces sugerido como líder de AntiSec, no planeó realmente las operaciones ni tampoco impartía las órdenes (de hecho, durante este período se mostró bastante disperso, aunque más tarde veremos que acudió a Hammond con solicitudes de hackeo específicas). El equipo principal de AntiSec en pleno trabajaba a veces al unísono, pero era más habitual que se dividiesen en grupos más pequeños para las distintas operaciones. Por ejemplo, se creó un canal secundario para hackear a la empresa de seguridad ManTech. Algunas de las operaciones disidentes nunca incluyeron a Sabu y sus aportaciones raramente eran de carácter técnico.

Sin embargo, Sabu desempeñaba dos funciones vitales. Era el hombre clave para la mayoría de exploits y datos de inteligencia que se transmitían al equipo y se convirtió en su cara visible. Mientras que Topiary actuaba a modo de embaucador en su manejo de las relaciones públicas para LulzSec, Sabu funcionaba para AntiSec más bien como un representante estable. Tomemos el siguiente tuit de 20 de junio, escrito pocas semanas después de

su arresto: «Operación Anti-Security: pastebin.com/9KyA0E5v– La mayor operación unificada entre hackers de la historia. Todas las facciones bienvenidas. Somos uno.»

Un puñado de miembros de AntiSec animó también a Sabu a que asumiera un perfil público e independiente como individuo. Aquel verano, influido tanto por la incitación de AntiSec como por la presión directa del FBI, Sabu utilizó Twitter a destajo, lanzando un verdadero torrente de retórica revolucionaria. Gracias a su carisma, adquirió un estatus próximo al culto. Con el final de LulzSec, los embaucadores míticos desaparecieron de escena. Y si bien es indudable que Sabu se convirtió en una figura mítica, su estilo de presentación pública no era en absoluto el de un embaucador. Representaba, en cambio, el papel arquetípico del hacker revolucionario proscrito. En la época anterior a este período, en gran medida, le estuve evitando, pero finalmente, a mediados del verano, cuando alcanzó el máximo protagonismo, decidí que había llegado el momento de comunicarme con él.

Sabu

Era el Día de la Independencia de los Estados Unidos, el 4 de julio de 2011. Sentada en una habitación sofocante sin aire acondicionado en San Juan, Puerto Rico —la ciudad donde me crié— hacía verdaderos esfuerzos por acabar de leer una entrevista a Sabu (la primera con este célebre hacker) mientras las gotas de sudor me resbalaban por la frente.[226]

Con la firma de Samantha Murphy para la revista *New Scientist*, el artículo ofrecía la primera entrevista pública realizada a Sabu. Me sentía inútil porque yo, una de las expertas mundiales en Anonymous, ni siquiera había conseguido mantener una simple *conversación* con el cerebro del grupo. Había mantenido las distancias con él porque, para ser sincera, me sentía intimidada. Su disposición no era exactamente cariñosa y alegre. Antes de pasarse al bando de los federales, Sabu había mantenido un perfil mucho más bajo online y exudaba una especie de actitud revolucionaria poderosa; no se trataba de alguien con quien simplemente chateas. Los llamamientos de Sabu para que la gente se sublevase se dirigían rutinariamente a sus “hermanos” y “hermanas”. Durante las conversaciones

de chat en el IRC dejaba caer la palabra “negro” y, a diferencia de los trols, parecía emplearla sin ningún atisbo de ironía. En lugar de un adolescente blanco, rico, alienado que vivía en un sótano, Sabu sonaba a hermano endurecido en la calle. ¿Acaso era posible que su alienación e indignación fueran producto no de una anomia de clase media, sino de la pobreza, la marginación racial y una familia rota?

En la entrevista relataba una travesura llevada a cabo en 1999 en la que Sabu desfiguró algunos sitios web en un intento de reclamar el fin de la presencia militar estadounidense en la pequeña isla puertorriqueña de Vieques. Una vez acabada mi lectura de la entrevista, reuní el coraje suficiente para enviarle un mensaje privado:

<biella>: hola Sabu solo quería felicitarte por tu trabajo en Vieques
<biella>: soy de la isla y estuve bastante comprometida con la política medioambiental en otro tiempo

Esperé su respuesta durante lo que pareció una eternidad. Para mí fue como si el mundo se hubiese detenido, con las gotas de sudor congelándose en mitad de mi espalda. Pero, en realidad, me respondió casi al instante:

<Sabu>: guai

Luego:

<Sabu>: ¿cuál es tu objetivo? Veo tu nombre asociado a alimentar/chivar/escribir documentos sobre anonymous
<Sabu>: dime cuáles son tus verdaderas intenciones
<Sabu>: estoy interesado

Los pensamientos se arremolinaron en mi cabeza. En un escenario donde la reputación es tan importante, la insinuación de Sabu escocía. Ahora entiendo que su acusación fue un gesto astuto; erigió un marco que haría que me resultara difícil verle como a un posible chivato. En aquella época ni siquiera podía imaginar que pudiera estar trabajando para el FBI. La cuestión de cómo podría eludir sus acusaciones eclipsó cualquier otra consideración:

<biella>: Sabu solo soy una antropóloga

Un nanosegundo después de haber tecleado el mensaje me di cuenta de lo estúpido que probablemente sonaban esas palabra. Cualquiera que tenga unas nociones básicas sobre los chivatos sabe que existe una historia bien documentada de antropólogos que trabajan como agentes encubiertos de la CIA. Intenté recomponerme:

<biella>: me topé accidentalmente con Anonymous en 2008
<biella>: a través de la Cienciología
<Sabu>: ok

Eso tampoco había sonado tan bien:

<biella>: mi pasión es la política
<biella>: de modo que me gusta estudiar la política de los medios digitales
<Sabu>: lo entiendo

Y entonces dije algo que aún hoy hace que me estremezca:

<biella>: en términos de anon, estoy intrigada y también preocupada (FBI, mi ordenador, etc)
<biella>: tomo precauciones con mis datos, no recopilo cierta clase de información tampoco, lo que resulta frustrante pero es la única manera que veo de tratar este asunto
<sabu>: bien ¿para qué quieres recopilar datos?
<biella>: me preocupa oír que mi nombre está asociado a chivatos/FBI pero entiendo que viene con el paquete
<Sabu>: ¿Histórico?
<Sabu>: ¿investigación en ciencias sociales?
<biella>: diría que es una combinación de ambas

Le expliqué que mi intención no era revelar “delitos”. Estaba interesada más bien en entender la dinámica social. Aunque nuestra primera conversación fue bastante pobre, para mi sorpresa —y alivio— nuestras conversaciones a través del chat se volvieron más regulares y cordiales. Pensé que le había convencido de que mis intenciones eran honorables o bien que Sabu les había preguntado por mí a otros miembros de AntiSec. Al

llegar a este punto estaba segura de que había informantes en AnonOps, pero en junio y julio muy poco rumores señalaban a Sabu como un topo, mientras que a menudo otros miembros importantes de Anonymous se veían acosados por las acusaciones. Mis conversaciones con Sabu no hicieron más que alimentar mi paranoia. El 23 de julio me preguntó:

<Sabu>: estás muy metida en los canales y comentarios de anonymous
<Sabu>: ¿nunca te visitan los federales?
<biella>: todavía no
<biella>: tampoco me han parado en la frontera aunque viajo sin mi ordenador o sin ningún ordenador, aunque tampoco es que haya nada que pueda incriminarme
<biella>: hay algo que me preocupa, tengo contactos con la EFF [Electronic Frontier Foundation]

Al igual que en mi primera conversación con Sabu, cuando le elogié con la esperanza de que hablara conmigo, él en cambio comenzó a alabarme a *mí*, incluso dándome las gracias:

<Sabu>: por todo el trabajo que haces
<Sabu>: en serio mucho respeto [en español en el original]
<Sabu>: a fin de cuentas este movimiento puede ser alucinante

Sabu también empezó a insinuar que el FBI me estaba vigilando:

<Sabu>: ... solo porque eres legal no significa que no te estén siguiendo

Era listo: el problema potencial era yo, no él. Sabu señaló este hecho en repetidas ocasiones y luego continuó con su retórica revolucionaria. Hizo que resultara muy difícil verle como otra cosa que no fuese un activista apasionado, inquebrantablemente comprometido con la causa.

Los placeres del secretismo

Pocas semanas después de mi primera conversación con Sabu, me invitaron a participar en un canal secreto de IRC para asistir a una única conversación entre miembros de AntiSec. Los participantes incluían a un puñado de

operadores de IRC de AnonOps y a Emmanuel Goldstein, el editor de la publicación hacker *2600* y presentador de un programa de radio para hackers llamado *Off the Hook*. Estos hackers se reunieron para evaluar si Goldstein estaría interesado en prestar su apoyo al subproyecto AntiSec orientado hacia la propaganda y la creación artística llamado "voz". Y aquí estaba yo, invitada al santuario interno. Observé intensamente mientras el grupo de unos veinte participantes debatía los méritos de la acción directa y el objetivo del proyecto voz.

Sabu fijó la agenda: «muy bien caballeros, vamos a incorporar a Emmanuel. Él será la voz de anonymous y antisec en la radio y realmente quiere ayudar a impulsar #voice.» Resultó que Goldstein no había hecho esas promesas y, mientras que muchos de ellos parecían estar abiertos a su participación, otros se opusieron de inmediato. Algunos le acusaron de ser un soplón. Ahora bien, uno debe entender que los rumores de chivatazos forman parte del ruido de fondo entre los hackers, que el propio ruido se convierte en una de las principales barreras contra la justificación de las reclamaciones. Durante la conversación de chat, un crítico observó que «*2600* tiene una historia de condena de los ataques, incluido cuando Anonymous doseó a mastercard y otros para wikileaks».

Adrian Lamo, el hacker que delató a Chelsea Manning, en algún momento había estado activo en el escenario de *2600*, con acceso a una cuenta del servidor de correo electrónico/shell de la revista. Según algunos, Lamo no había sido suficientemente purgado. Muchos estaban furiosos por esta cuestión, así como con la convención de Hackers on Planet Earth (HOPE), organizada por Goldstein y un numeroso equipo y en cuyo panel estaba Lamo.

Yo estaba particularmente intrigada por lo que una figura llamada Anarchaos estaba escribiendo en aquella sala de chat. No era nadie que hubiera visto antes online y así seguiría durante un par de meses más antes de que pudiera conversar con él por primera vez y bajo un handle diferente. Goldstein empezó a cuestionar las tácticas como los ataques de DDoS y la organización de manifestaciones callejeras de bloque negro (táctica de manifestación donde los participantes llevan ropa negra para evitar ser identificados por las autoridades y parecer una masa uniforme) y Anarchaos defendió incondicionalmente su legitimidad. «Tengo razones políticas y personales para asumir una acción directa contra las fuerzas que nos

oprimen. Que no se piense que aquellos que luchan con la fuerza no lo hacen con el cerebro.» Los participantes de Anons en el canal admitieron que «somos más que capaces de lanzar ataques altamente sofisticados pero, cuando estamos en las trincheras disparando contra nuestros enemigos, no necesitamos que otros llamados hackers socaven nuestros esfuerzos». Más tarde alguien añadió que «la diversidad de tácticas es la manera más efectiva de ganar campañas»".

Lo que había comenzado como una conversación fascinante sobre las diversas tácticas que se pueden emplear explotó rápidamente en un festival de antorchas. En un momento dado alguien preguntó a Goldstein si alguna vez me había conocido (no lo había hecho). Aproveché la atención que de pronto se dirigía hacia mí para compartir con él mis ideas acerca del panel de HOPE que incluía a Adrian Lamo. Escribí que era «alucinante» y que estaba «encantada de que lo hayas organizado».

«No te imaginas la presión que tuve que soportar para NO hacerlo», contestó Goldstein. Alguien en la sala de chat aprovechó la oportunidad para afirmar que todavía estaban cabreados: «Lamo no debería ser bienvenido a ningún encuentro de hackers y no es más que otro clavo en el ataúd para que muchas personas rechacen a la gente de *2600* por traidores.»

La conversación volvió brevemente a la cuestión de si *2600* podía contribuir al proyecto voz antes de pasar al "lame-ass flaming" (insultos a *lame-ass*, culo aburrido, jugando con *Lamo*), como lo describió uno de los participantes. Goldstein decidió marcharse: «Lamento provocar un tono tan agrio, de modo que me largo. Pero estamos abiertos al diálogo.» El proyecto voz se lanzó poco después en un canal de IRC público, sin la ayuda de Goldstein. Aunque el propósito del encuentro había fracasado, sirvió para confirmar lo que yo sospechaba: que el equipo de AntiSec incluía numerosos hackers, como el caso de Anarchaos, que estaban activos pero ocultos. ¿Quién era esa gente? ¿Por qué no les había visto antes? Los principales participantes de LulzSec, como Topiary, tflow y Sabu, eran en su mayoría figuras muy conocidas. Estaba claro que Anonymous, un colectivo de por sí bastante esquivo, estaba protegido debajo de todavía más capas de secretismo.

Y yo también era arrastrada cada vez más hacia esta órbita de secretismo. Había tratado de mantener la distancia respecto de los canales donde se organizaban actividades ilegales. Cuando hablaba privadamente

con Anons les pedía a menudo que se ahorrasen los detalles que pudieran resultar incriminatorios (sabiendo que ellos podían tener el impulso de jactarse de alguna acción épica relacionada con la seguridad). Les dejé claro a todos que mi función como antropóloga significaba que tomaba notas con frecuencia, guardando algunas partes de los archivos, y en caso contrario reuniendo información. Aunque encriptaba los datos, yo no mantenía ningún privilegio especial que pudiera impedir que se me considerase como cómplice de un delito. Como consecuencia de esta situación no me invitaban a los canales secretos y yo (en buena parte) evitaba las historias presuntuosas relativas a hackeos ilegales. Mi actitud era también siempre honesta y creo que eso contribuyó a que la gente entendiese qué era lo que buscaba; una verdadera rareza en una cultura que se caracteriza por la desconfianza, la sospecha, los rumores y el miedo. Pero parecía que ahora las cosas estaban cambiando. Me estaba deslizando hacia zonas más profundas y oscuras de este laberinto, con un acceso fugaz a conversaciones privadas y con la creciente preocupación de que eso pudiese convertirse en un problema.

En una ocasión, Aldous Huxley escribió: «Asociarse con otras personas afines en grupos pequeños y determinados es para la gran mayoría de hombres y mujeres una fuente de profunda satisfacción psicológica. La exclusividad se añadirá al placer de ser muchos, pero uno; y el secretismo lo intensificará hasta alcanzar casi el éxtasis.»[227] Para los hackers que participaban en Anonymous el secretismo era, sin lugar a dudas, una de las razones principales de aquello que les hacía volver a por más. El secretismo proporcionaba una suerte de sostén a esta comunidad underground. Y si bien la palabra “éxtasis” podría ser demasiado fuerte cuando se aplica a mi caso, no puedo negarlo: la aceptación dentro de esta sociedad esotérica me proporcionaba un emocionante subidón de contacto.

¿Dónde estás tú, Anonymous?

Aunque al principio era emocionante permanecer en las sombras en compañía de Anonymous, a comienzos de agosto de 2011 mi estado de ánimo se había deteriorado. El ritmo frenético de la actividad de Anonymous se había convertido en algo nuevo a través de la pura

militancia en las operaciones. Empecé a preguntarme en qué momento el FBI o cualquier otra agencia del gobierno atraparía a más Anons o incluso me haría una visita. AntiSec, al igual que antes LulzSec, había adoptado un ritmo de hackeo casi constante, generando abrumadores comunicados que simplemente pedían a gritos una reacción del Estado: #FuckFBIFridays, #ShootingSherrifsSaturday, #MilitaryMeltdownMonday.

AntiSec doxeó las oficinas del sheriff, desfiguró y destruyó sitios web de la organización policial, como el de la California Statewide Law Enforcement Association, y filtró información personal de los jefes de policía de Nueva York. Solo en el mes de julio atacaron los sitios web de setenta y siete organismos de seguridad diferentes (todos alojados en el mismo servidor). Descargaron un gigabyte de datos de las Vanguard Defense Industries y consiguieron a través del hackeo la cuenta de correo electrónico de uno de sus vicepresidentes ejecutivos. Estos hackers le revelaron al mundo los documentos que habían “obtenido” incluida una propuesta al FBI del contratista de defensa IRC Federal para un proyecto llamado Proyecto Especial de Modernización de Identidades (SIM), cuya finalidad era identificar a aquellas personas que “pudieran” representar un riesgo criminal o terrorista en el futuro. Afirmaron haberse infiltrado en numerosas redes internas del Departamento de Energía de los Estados Unidos, donde enviaron mensajes instando a los empleados a trabajar contra el gobierno en lugar de para él. Hackearon asimismo a la empresa contratista federal ManTech International, haciendo públicos casi cuatrocientos megabytes de contenido que detallaba sus negociaciones con la OTAN y con el ejército estadounidense (junto con los correos electrónicos de todos sus empleados). Atacaron a la empresa contratista de mega-seguridad Booz Allen Hamilton; aunque no consiguieron obtener documentos reales —aunque uno de los empleados de Booz Allen Hamilton en aquella época, Edward Snowden, finalmente lo hizo—, se las ingeniaron para descargar noventa mil correos electrónicos militares del sitio de la empresa, que volcaron en Pirate Bay junto con un extenso análisis donde señalaban “hechos clave” de la empresa, como el desglose de su financiación. Las cosas habían tomado un giro realmente serio.

Durante este estallido de actividad, los arrestos se volvieron habituales. Hacia finales de julio, catorce estadounidenses fueron arrestados por dosear a PayPal, y las autoridades británicas detuvieron a dos miembros de

LulzSec: Topiary en Escocia y tflow en Londres (el nombre de tflow no se hizo público en esa época porque aún era menor de edad). Justo antes de su arresto, Topiary dejó una sentencia que hoy se encuentra solitaria en su eliminada cuenta de Twitter: «No puedes arrestar una idea.»[228]

Era un verano caluroso. En este clima de peligro y amenaza empecé a sufrir pesadillas cada semana en las que agentes especiales del gobierno aporreaban mi puerta. Me preguntaba dónde diablos me había metido, y no era la única. Durante una entrevista, un Anon manifestó su sorpresa: «Ninguno de nosotros sabía que se encontrarían así... encerrados durante décadas, huyendo, en el exilio, suicidios, enfermedades mentales ptsd [*sic*] etc., etc.» Los Anons se acercaban cada vez más a mí con confesiones de sentir miedo y alimentando así mi creciente inquietud. El 1 de agosto alguien me encontró y escribió que «la mierda se está volviendo EXTREMADAMENTE peligrosa atm [en este momento] ... para aquellos que están en AntiSec por ejemplo». Al día siguiente, otro hacker me dijo, «un helicóptero aterrizó a la 7 de la mañana en un campo junto a mi casa. El corazón se me puso a 200 hasta que me di cuenta de que se trataba de una fumigación de cultivos». Entre la gente que me asustaba en privado, la ola de arrestos, mi vida suspendida mientras dedicaba cada vez más tiempo a la investigación, la interactividad bajo seudónimos basada en textos y altamente intermediada, y los crecientes tentáculos del secretismo, me sentía frustrada y quemada. Todo este asunto me estaba afectando. Me preocupaba el futuro de Anonymous, mi propio futuro y las vidas de los que habían sido arrestados. Algunos hackers en AntiSec comenzaron a notar que mi ánimo estaba por los suelos. Algunos se pusieron en contacto conmigo en privado, animándome a que no tirase la toalla. Uno de ellos me dijo que si abandonaba me perdería algunas cosas «realmente especiales».

No me molesté siquiera en preguntar cuáles podrían ser esas cosas especiales. Las filtraciones y los compromisos seguían siendo fuertes, pero habían perdido su brillo. Para mí, #FuckFBIFridays y #MilitaryMeltdownMonday habían empezado a convertirse en #FuckFBIFatigue y #MyMeltdownMondays. También me frustraba el hecho de que, mientras que mi acceso a AntiSec iba en aumento, parecía surgir más actividad por parte de otros grupos de hackers más pequeños de los que apenas si conocía su existencia. Los días de las insurrecciones a gran escala de Anonymus están siendo eclipsados. Anonymous había sido

una experiencia emocionante para mí por una razón específica: era el movimiento comunitario problemático más grande y popular que Internet había fomentado hasta entonces. Pero, de pronto, parecía que AnonOps/Anonymous se estaba deslizando hacia un estado más familiar de hacker-vanguardismo. Y eso significaba, desde una perspectiva puramente logística, que Anonymous se estaba convirtiendo en un objeto de estudio mucho más complicado.

Analizado retrospectivamente, existe al menos una explicación concreta para la creciente fragmentación de Anonymous: la interferencia directa del gobierno. Gracias a las mega filtraciones de documentos de la ANS hechas por Edward Snowden en 2013, sabemos que, en verano de 2011, el Cuartel General de Comunicaciones del Gobierno británico (GCHQ) apuntó a la infraestructura de comunicaciones de AnonOps. Una unidad especial del GCHQ llamada Grupo Conjunto de Inteligencia e Investigación sobre Amenazas (JTRIG) —que también participa en intromisiones estilo COINTELPRO— lanzó ataques DDoS contra Anonymous bajo el nombre de "Op WEALTH" y "Rolling Thunder".[229]

Fue la primera ocasión conocida de un gobierno occidental que utiliza secretamente ataques de DDoS —criminalizados tanto en el Reino Unido como en Estados Unidos— como una táctica contra sus propios ciudadanos. El GCHQ declaró que su operación había sido un éxito; las diapositivas filtradas alardeaban de que, como resultado de su doseo al IRC de AnonOps, «el 80 por ciento de los que enviaron mensajes no estavan[*sic*] en los canales de IRC un mes más tarde». Para entonces, el gobierno británico ya había arrestado a los participantes británicos por el mismo hecho. Uno de los arrestados, Chris Weatherhead, alias "Nerdo", era un operador esencial y muy apreciado de AnonOps. Finalmente recibiría una condena de dieciocho meses por su participación en la campaña de DDoS "Vengar a Assange/Operación Venganza". No se le consideró culpable de haber participado propiamente en un ataque de DDoS concreto, sino de colaborar en la operación gestionando el servidor de IRC. El gobierno británico, por otra parte, no había recibido ninguna sanción por dosear a los activistas. La ley, claramente, no se aplica de la misma manera. Tal como lo expresó Weatherhead en Twitter cuando leyó la noticia: «Mi gobierno utilizó un ataque DDoS contra servidores que yo gestionaba y después me acusó de dirigir ataques de DDoS. En serio, ¿de qué coño van?»[230]

Con este enfoque la justicia pulveriza su castigo sobre miles de personas que participan en debates y protestas, simplemente porque un puñado de ellas ha cometido actos de vandalismo digital.

Esta tentativa de disuasión puede haber contribuido a paralizar las acciones de Anonymous en general, pero no tuvo ningún efecto para detener a AntiSec. Ellos funcionaban en una red de IRC diferente. Si bien algunos de sus miembros fueron efectivamente arrestados, y otros abandonaron por diversas razones, el consenso general era que, como me dijo uno de los miembros de AntiSec, «no hay vuelta atrás».

Necesitaba tomarme un descanso. Reservé un viaje para asistir a una de las conferencias de hackers más famosas del mundo, el Chaos Communication Camp, organizada por el Chaos Computer Club cada cuatro años en Alemania. Pensé que pasar un tiempo sin conectarme, con hackers a los que conocía, con amigos —o al menos con personas a las que realmente podía *mirar*— atenuaría la sensación de vértigo que se había instalado en mí.

Sin embargo, después de una sucesión de días y noches en el festival hacker y un vuelo a primera hora desde Alemania, regresé a Estados Unidos más agotada que antes de emprender el viaje. El espíritu de Anonymous, en cambio, parecía haberse renovado. Mientras me dirigía a recoger mi equipaje vi una imagen que me resultó familiar en una lejana pantalla de televisión: la máscara de Guy Fawkes. Di un respingo y me dirigí rápidamente hacia el monitor. La cadena CNN estaba mostrando un tuit en el que se hacía un llamamiento a la “OpBART” (“BART” significa Bay Area Rapid Transit). A partir de las pistas visuales proporcionadas por la CNN comprendí que esta operación no solo era importante. Parecía encajar en el patrón de los levantamientos de la vieja escuela, tumultuosos y a gran escala, característicos del Anonymous previo a AntiSec. El 80 por ciento de los usuarios que el GCHQ supuestamente había eliminado con sus ataques de DDoS habían regresado, junto con centenares de recién llegados.

El punto de origen de la OpBART se remonta al 3 de julio de 2011, cuando la policía del BART hirió de muerte a Charles Hill, en la estación del BART de Civic Center de San Francisco. Aunque el hombre estaba borracho e iba armado con un cuchillo, muchos pensaron que matarle había sido un uso excesivo de la fuerza. También fue un recordatorio del problema general que entrañaba la brutalidad policial. En 2009, la policía

había matado a un afroamericano, Oscar Grant III, en la estación BART de Fruitvale de Oakland. Los policías le dispararon por la espalda mientras le retenían en el suelo. En respuesta a la muerte de Hill, los organizadores locales convocaron una marcha de protesta el 11 de julio. Alrededor de un centenar de manifestantes interrumpieron el servicio de BART en la estación de Civic Center. Al mes siguiente se convocó otra protesta en el mismo lugar. En esta ocasión, los agentes de BART decidieron bloquear la señal de recepción de los teléfonos móviles en las estaciones para impedir la manifestación de agosto. El portavoz de BART, Linton Johnson, explicó sus razones a la CNN: «Tomamos una decisión dolorosa obligados por la actitud de los manifestantes... [los activistas] nos obligaron a elegir entre la capacidad de la gente para utilizar sus teléfonos móviles [y] su derecho constitucional a ir del punto A al punto B.»[231]

La última vez que lo comprobé, la Constitución protege tanto la libertad de expresión como la libertad de asociación, pero no la libertad de transporte. Los geeks de Anonymous, que conocen muy bien los derechos constitucionales, naturalmente se enfadaron. Jackal, el principal encargado de la cuenta de Twitter @YourAnonNews, inauguró públicamente #OPBART con una serie de mensajes cáusticos. Tenía más de 300.000 seguidores, y poco después de ser presentada en la CNN, la cuenta sumó otros 200.000 (lo que también precipitó la visita del FBI a Jackal). Anonymous y otros ciudadanos preocupados contaban con el ingenioso hashtag “#muBARTec” para relacionar este acto de censura con el apagón de telecomunicaciones a gran escala impuesto por el expresidente egipcio Hosni Mubarak apenas unos meses antes, en enero de 2011.

Jackal trabajaba con un pequeño equipo. Mantenía un rincón semiprivado, un canal de IRC llamado “la cabaña”, que inicialmente incluía solo a cuatro individuos. Concebido principalmente como un espacio social, uno de los primeros miembros añadió el término “cr3w” al nombre, burlándose ligeramente del LulzSec y de las otras autoproclamadas “tripulaciones” que en aquella época surgían como setas. La Operación BART, su primera operación real, transformó accidentalmente a CabinCr3w de un canal social en un equipo prolífico y activo. En los meses siguientes, su número aumentaría hasta incluir a unos veinte participantes. Llegarían a ser conocidos como especialistas en extracción de datos de código abierto, que buscaban y filtraban material a través de las bases de datos

proporcionadas por otros hackers que se infiltraban en los servidores en busca de información (si bien algunos hackers de CabinCr3w, como Kahuna [John Anthony Borell III], y w0rmer [Higinio O. Ochoa III] también participaron en intrusiones digitales y fueron arrestados más tarde).

Pero a mediados de agosto, justo cuando OpBART empezaba a actuar, el equipo seguía siendo reducido. Y debido a que su mano de obra era escasa, los primeros tres días los participantes tuvieron que trabajar día y noche. A través de Facebook, CabinCr3w se conectó con los residentes para organizar protestas callejeras y se unió a la amplia comunidad de Anon, poniéndose en contacto con algunos organizadores consolidados. Un canal público en IRC, #opbart, se convirtió en un punto de encuentro en el servidor de AnonOps. Todo el mundo se puso manos a la obra redactando material de propaganda para anunciar la protesta prevista para el lunes 15 de agosto. De un modo ya conocido desde la Operación Vengar a Assange, los organizadores actuaron a modo de coreógrafos —para usar el acertado término acuñado por Paolo Gerbaudo— que utilizaban y dirigían un cañonazo de furia.[232]

Junto a las manifestaciones de protesta y la propaganda, algunos individuos participaron de un comportamiento bastante peligroso, aunque reconocidamente imbuido de lulz; fueron estos actos los que atrajeron la atención de los medios de comunicación más importantes.

Por ejemplo, alguien que decía pertenecer a Anonymous encontró una fotografía picante de Linton Johnson, el portavoz de BART, en su sitio web personal, en la que aparecía semidesnudo. Esta fotografía fue reeditada en el sitio web “bartlulz” —con una considerable fanfarria— acompañada de la siguiente impúdica racionalización: «si vas a ser un capullo para el público, seguro que no te importará enseñarle la polla ... Umad Bro? #Bartlulz.»[233]

Pero, más que cualquier otra cosa, fue una sucesión de hackeos lo que suscitó la cobertura de los medios de comunicación nacionales, desde la CNN hasta *Democracy Now*!

En primer lugar, el 14 agosto se produjo una desfiguración de un sitio web. Los intrusos simplemente desfiguraron myBART.org con una imagen de Guy Fawkes. A esta acción le siguió una intrusión casi inmediata que revelaba los datos privados de 2.500 clientes de BART. El 17 de agosto, al día siguiente de la segunda protesta ante la estación de BART de Civic

Center organizada por Anonymous y activistas locales, se produjo otra intrusión a un sitio web del sindicato policial de BART. Esta acción desencadenó la publicación en Pastebin de los domicilios particulares, direcciones de correo electrónico y contraseñas de 102 agentes de policía de BART, entre otros empleados.

El día que regresé de Alemania, la gente de *Democracy Now!* se puso en contacto conmigo para pedirme que me reuniera con ellos al día siguiente para hablar sobre OpBART. Me inquietaba que me pudieran preguntar sobre las flagrantes violaciones de la privacidad cometidas por esos hackeos y por las maniobras necesarias para explicar el empleo de dichas tácticas por un colectivo que claramente luchaba para proteger esa privacidad. Afortunadamente, al día siguiente se me unió en directo por televisión un activista de Anon enmascarado, Commander X, y fue a él a quien se le pidió que diese las razones de ese comportamiento:

> AMY GOODMAN: ¿Y su opinión... sobre el hecho de perseguir a los propios pasajeros, a gente que podría no desear que se revelase su información personal?
>
> X: ¿... De qué otra manera se consigue que el mundo reaccione y asegure vuestra información? ¿De qué otra manera se consigue que estas empresas y estos grandes gobiernos mantengan vuestra información, la información que les proporcionáis voluntariamente, segura? Creo que logramos transmitir nuestro mensaje y os apuesto una cosa: apuesto a que la próxima vez lo arreglarán.[234]

Commander X, que hablaba a través de un distorsionador de voz, no era el responsable de la infracción, pero el presunto autor y una minoría de otros hackers compartían su argumentación. En aquel momento no tenía ni idea de quién estaba detrás de esos hackeos y tampoco de cómo veían otros Anons esta infracción. Pero poco después de la entrevista regresé a casa y lo descubrí.

Aunque en Anons existía un apoyo enorme —casi unánime— a la protesta por el acto de censura de BART, el hackeo y posterior filtración de los datos de los clientes fue una de las acciones más internamente divisivas que había visto hasta entonces. Las conversaciones en los canales, e incluso

públicamente en Twitter, rebosaban de críticas.

Echemos un vistazo, por ejemplo, a lo que sucedió cuando Lamaline_5mg se conectó al canal público OpBART el 17 de agosto y se hizo responsable del hackeo al sitio web del sindicato policial de BART. Ella ofreció un enlace al material doxeado:

<Lamaline_5mg>: Hola a todos
<CrappyTIres>: Hola Lamaline_5mg
<Lamaline_5mg>: tengo una pequeña contribución.
<Lamaline_5mg>: http://pastebin.com/XX7DJBqw
<Lamaline_5mg>: Una filtración de http://bartpoa.com/ [Asociación de Agentes de Policía de BART]
<Lamaline_5mg>: Disfrutad y compartidlo.
<CrappyTIres>: hmm a *CrappyTIres no le gustan las filtraciones de información
<OpNoPro>: ¿esos nombres han sido compartidos alguna vez?
<Lamaline_5mg>: ¿Qué?
<Lamaline_5mg>: No lo sé. Supongo que no.
<OpNoPro>: Filtraste nombres y contraseñas
<OpNoPro>: Aquí dirigimos una operación muy limpia
<OpNoPro>: No estamos interesados en esa clase de cosas
<OpNoPro>: Por favor, debes abstenerte de filtrar información privada de nadie en ningún sitio en nombre de anonymous... no estamos interesados en violar la privacidad de nadie... ellos tiene tanto derecho a ella como tú

Pero no todo el mudo estaba de acuerdo con OpNoPro. Otros apoyaban decididamente las maneras de sombrero negro empleadas por AnonOps:

<sharpie>: es su mierda
<OpNoPro>: haz tu trabajo privadamente y nadie necesita saberlo
<sharpie>: cierra la puta boca
[...]
<Lamaline_5mg>: No tengo la culpa de que su seguridad sea una mierda.
<OpNoPro>: Tranquilo pluma afilada [sharpie]
<OpNoPro>: No es una cuestión a debate
<OpNoPro>: es una cuestión de mantener las cosas separadas
<sharpie>: la gente piensa que este irc es un puto grupo de ganchillo de la parroquia
<OpNoPro>: Por favor entiende la situación
<sharpie>: sí
<sharpie>: la entiendo
<sharpie>: mucho más que tú

<OpNoPro>: Hay muchas partes del IRC *CrappyTIres que buscan el grupo de ganchillo
<OpNoPro>: Tranquilo pluma afilada
<OpNoPro>: Despierta
<OpNoPro>: mantén las cosas separadas
[...]
<sharpie>: coge tu mierda moralista de sombrero blanco y métetela donde te quepa
<OpNoPro>: Y si alguna vez me ves en un club de ganchillo será una ilusión óptica
<OpNoPro>: No tienes idea de cuál es mi moral

Sharpie acabó el intercambio recurriendo a uno de los argumentos más comunes:

<sharpie>: ¿cuánta publicidad crees que habría tenido "#opbart" sin las putas filtraciones?

Y entonces Lamaline_5mg dijo que ella ni siquiera pertenecía a Anonymous, planteando la cuestión ontológica de qué es lo que te convierte realmente en Anonymous. Ella apareció en el servidor de IRC de Anonymous, ofreció material doxeado y luego procedió a trabajar con otros Anons para redactar un comunicado de prensa; si eso no te convierte en un Anon, ¿entonces qué lo hace? Además, esta distinción importaba muy poco en relación a las cuestiones éticas más generales que rodeaban al hackeo y al doxeo. Hasta entonces, gracias a AntiSec, estas tácticas eran un elemento común en el paisaje de Anonymous y no haría más que volverse más polémico:

<Lamaline_5mg>: Esto no es anonymous.
<Lamaline_5mg>: Que te jodan.
<w>: OpNoPro, te guste o no, el caos fractal y la diversidad en las tácticas es lo que está alimentando la revolución global
<AlbaandOmegle>: Anon crea problemas
<AlbaandOmegle>: porque funciona
<OpNoPro>: llévate tus filtraciones a otra parte
<w>: OpNoPro, no puedes impedir que la gente utilice el nombre de una operación para doxear, dosear y hackear
<w>: OpNoPro, aunque fuera la opción correcta, simplemente no puedes hacerlo
<Lamaline_5mg>: no uso el nombre de la operación.

Las versiones de esta conversación se repetirían al menos una docena de veces en otros lugares durante los días siguientes. Mi lectura fue que la mayoría de los participantes en AnonOps se oponían a las filtraciones que violaban datos privados, pero se mostraban mayoritariamente partidarios de apoyar otras tácticas ilegales, como la desfiguración del sitio web de BART, el bombardeo de correos electrónicos y mensajes de fax y el doxeo (independientemente del hecho de que fracasaran; BART había puesto en práctica una protección eficaz contra los ataques de DDoS). Una minoría apoyaba el doxeo simplemente porque servía al objetivo superior de concitar la atención de los medios de comunicación, o era un ejemplo del "caos fractal" que definía parcialmente a Anonymous.

El doxeo marcó también la primera vez que las sospechas de una "operación de bandera falsa" surgieron extensamente dentro de Anonymous. Una operación de bandera falsa es una intervención secreta, encubierta, en la que un agente del gobierno lleva a cabo una acción controvertida en nombre de un grupo político con el propósito de sembrar la desconfianza y la polémica o proporcionar una justificación para la propia respuesta intensificada del gobierno.

Dos días más tarde, Lamaline_5mg publicó una declaración en Pastebin que pareció avivar los rumores de una bandera falsa, aunque hizo muy poco para acabar con la controversia:

> Me parece vergonzoso que los medios de comunicación no condenen las medidas tan drástica contra una protesta después del *asesinato* de un ciudadano inocente. No se había demostrado que era culpable, ¿o caso realmente juzgan a la gente en su funeral? Suponiendo que este tío haya recibido un funeral apropiado.
>
> También encuentro inquietantemente triste que los medios de comunicación locales del Área de la Bahía de San Francisco se muestren tan comprensivos con el derecho al anonimato del personal policial de BART cuando les importó una mierda que este hombre fuese asesinado.
>
> ¿Condenaron acaso el asesinato de ese hombre?

> Todo lo que hice fue darles (a los policías) un poco de su propia medicina, es decir, 'Lamaline' que es un analgésico (por vía anal)... (Buscadlo)
>
> También significa «La ingeniosa» en francés.[235]

En una entrevista posterior con *SF Weekly*, Lamaline_5mg afirmó ser francesa, mujer y preadolescente (los dos últimos datos poco probables). Añadió que el hackeo de BART era su primera intrusión.

En medio de todo este asunto, un mensaje colgado en pastebin.com titulado «Anonymous NO es Unánime» fue recogido y leído por muchos participantes:

> Anonymous tiene un problema de percepción. La mayoría de las personas cree que somos un grupo de hackers oscuros. Éste es un error fundamental. Anonymous son *grupos* de hackers oscuros y aquí reside el problema. Anonymous ha hecho muchas cosas buenas en los últimos nueve meses. Ha contribuido junto con otros grupos a ayudar a la gente sobre el terreno en países donde "democracia" es una mala palabra.
>
> Los principales medios de comunicación necesitan entender que Anonymous no es unánime. Aun no he visto ningún informe a gran escala que haga esta distinción. Una minoría destructiva consigue la mayor atención de la prensa, mientras que a aquellos de nosotros que trabajamos en la sombra haciendo el bien a la gente en nuestro país y en el extranjero nadie nos lo agradece.[236]

Esta declaración refleja el compromiso de Anonymous con la diferencia, la pluralidad y la disensión, una formulación similar al tipo de política antagonista promovida por la teórica radical Chantal Mouffe.[237]

A menudo, Anons discrepa y participa en una intensa guerra de palabras. Pero dedica escasa energía a intentar eliminar sistemáticamente la diferencia, o a generar alguna solución "intermedia". En cambio, las diferencias se manifiestan ruidosamente, se escuchan, se responden y se aceptan a regañadientes. Anons reconoce ampliamente que no se puede

hacer nada drástico o significativo para eliminar las diferencias y continúan con sus intervenciones o, si los desacuerdos son insoportables, se separan para constituir un nuevo nodo.

Que se joda AntiSec

La controversia suscitada por el hackeo de OpBART finalmente remitió. Pero una controversia siguió presente. A medida que pasaban las semanas y los meses aumentaban las críticas a los hackeos y desfiguraciones llevados a cabo por AntiSec, aun cuando la base de apoyo al grupo crecía. Algunos Anons consideraban que AntiSec era un grupo irresponsable y muchos sospechaban de sus motivos. Circulaban rumores de que no solo las acciones particulares, sino también la totalidad de AntiSec podían ser una operación de bandera falsa.

AntiSec, como quizás cabía esperar, era un grupo respetado, tolerado y vilipendiado a partes iguales. Muchos de los principales miembros de AntiSec habían sido piezas fundamentales para las iteraciones pasadas de la constelación Anonymous/AnonOps/LulzSec. Su importancia coincidió con la desaparición parcial de WikiLeaks, una organización que sufrió las consecuencias de las fricciones internas y los problemas jurídicos. Se creía que AntiSec se podría expandir y desafiar de un modo más directo a los poderes protegidos por corporaciones y gobiernos —no simplemente mediante la producción de espectáculos pasajeros, como es el caso de los ataques de DDoS, sino también a través de denuncias—, localizando y revelando pruebas flagrantes de mala conducta.

A pesar de los hackeos constantes lanzados durante el final del verano y principios del otoño de 2011, fue muy poco lo que se pudo revelar que tuviese realmente sustancia. (Si Sabu no hubiese sido un informante del FBI es probable que AntiSec hubiera podido proporcionar más información. El FBI advirtió a algunas empresas de las violaciones de seguridad, lo que impulsó así la rápida reparación de los fallos y cerró eficazmente las puertas que AntiSec acababa de abrir.) Un Anon que había estado profundamente implicado desde otoño de 2010 se marchó en agosto de 2011, molesto en gran medida con las actividades de AntiSec. Aunque LulzSec volcaba gran número de datos —tales como nombres de usuarios, direcciones de correos

electrónicos, contraseñas, correos electrónicos y otros documentos— se consideraba que gran parte de ese material carecía de peso político. Y, sin embargo, AntiSec conseguía mantenerse en el centro del escenario. La gente empezó a resentirse de esta situación. Había muchos equipos pequeños operando, muchos de ellos fuera del ojo público. Se planteó la posibilidad de que AntiSec se hubiera vuelto contraproductivo y canalizara atención, trabajo y recursos hacia actividades que no tenían ninguna utilidad. Otro hacker que había sido miembro principal del personal de IRC de AnonOps me explicó: «Nos cabreó que nos lanzaran AntiSec por la cabeza. No recibimos ningún aviso. Y llevaban tiempo planeándolo, reclutando a gente de aquí.»

Peor aún, AntiSec comenzó a provocar polémicas entre algunos Anons a causa de un antiguo y respetado tabú de Anonymus: la búsqueda de fama. Un Anon expuso esta visión en el IRC en septiembre de 2011 durante su dimisión del grupo (se ha cambiado el seudónimo):

<ha>: qué coño pasó con #antisec
<ha>: permitidme que os cuente una historia
<ha>: acercaos chicos
<ha>: había una vez un equipo de status fag hackers, la mayoría de los cuales estaban bien como personas, todos tenemos defectos. Llegaron a ser conocidos como lulzsec
<ha>: Estos hackers decidieron que sería una buena idea utilizar sus poderes de status fag para unir a anons contra la industria de infosec.
<ha>: Fue entonces cuando alguien decidió darles ametralladoras a los monos y enseñarles los puntos débiles de las tablas sql. Estos monos decidieron que querían dar una buena impresión a lulzsec y hackearon todo lo que pudieron, divulgando toda la información saqueada independientemente de aspectos tales como las consecuencias y la comunicación.
<ha>: Los datos privados se filtraron más rápido que un condón de la marca WikiLeaks.
<ha>: siguieron hackeando datos esperando la palmada a la espalda de Sabu.
<ha>: Entonces se acabaron las vacaciones de verano.
<ha>: Se encontraron incapaces de continuar sus hackeos ya que surgieron cuestiones más apremiantes, tales como con quién sentarse a la hora de comer y qué asignatura optativa es más guai, francés o tocar en la banda.
<ha>: Y así acaba la saga de #antisec

Aquel verano, la red de AnonOps se había vuelto tan crítica con Barrett Brown que él decidió dejarlo. Se mostró inflexible en su decisión de abandonar cualquier relación con Anonymous, centrando ahora su energía en el "Proyecto PM", un equipo wiki dedicado a documentar el funcionamiento interno de los contratistas privados que realizaban tareas de seguridad para el gobierno. Posteriormente, Brown volvió a ayudar a Anonymous en #OpCartel, una operación controvertida y peligrosa que tenía como objetivo a los cárteles mexicanos de la droga. Y también recibía información para el Proyecto PM de AntiSec, cuando el grupo finalmente se apropió de datos sensibles pertenecientes a una empresa de seguridad llamada Stratfor. Pero faltaban todavía varios meses para que ocurriese todo eso. En aquella época Brown seguía siendo un recordatorio de que querer llamar la atención no estaba bien visto.

La búsqueda de atención por parte de AntiSec era más ambivalente y complicada de lo que había sido en el caso de Brown. A diferencia de Brown, AntiSec buscaba llamar la atención bajo un manto pseudo anónimo. Y algunos Anons apoyaban las acciones del grupo, conservando la esperanza de que sus esfuerzos habrían de producir finalmente alguna información política, clasificada o secreta, imposible de obtener mediante procedimientos legales.

Un grupo de hackers de sombrero negro (no vinculados a Anonymous) ya había tenido suficiente con AntiSec. Un grupo de hackers underground que actuaba bajo el nombre de BR1CKSQU4D, que parecía que habían adoptado solo temporalmente, hizo público un documento que incluía algunos supuestos doxeos de miembros de Anonymous y AntiSec. Comenzaban declarando:

> !QUE SE JODA ANONYMOUS! ¡QUE SE JODA ANTISEC! ¡QUE SE JODA ANONYMOUS ! ¡QUE SE JODA ANTISEC! [238]

Más adelante, no se anduvieron con rodeos:

> ¿Y os preguntáis por qué los grupos de los noventa a los que mostrabais vuestro agradecimiento (con hijos y familias) no salen de su retiro para ayudaros?

> No habéis hecho más que exacerbar la retórica de la ‘guerra informática’ y provocar una legislación que acabará con condenas de 50 años de prisión para los hackers.
>
> La parte más retrasada es que ni siquiera os dais cuenta de que vosotros sois la causa de aquello que odiáis;
>
> Cada vez que lanzáis un ataque de DDoS contra una empresa, Prolexic o DOSarrest consiguen un nuevo cliente. Cada vez que aplicáis una inyección SQL a algún sitio irrelevante, una empresa dedicada a los tests de penetración consigue un nuevo contrato.
>
> Cada vez que declaráis la guerra informática al gobierno, los contratistas federales reciben una oleada de dinero procedente de subvenciones.

Otros hackers e internautas también empezaron a acusar a Anonymous de reforzar el complejo industrial de la guerra informática. Pero merece la pena señalar que mucho antes de que Anonymous alcanzara notoriedad, los gobiernos nacionales de todo el mundo ya aspiraban a controlar Internet y estaban elaborando estatutos que erosionaban los derechos y la privacidad individuales. Las iniciativas en ciberseguridad estarían bien financiadas con o sin Anonymous. Esto no significa que todas las acciones llevadas a cabo por el grupo estén justificadas. No obstante, a la luz de un estado de vigilancia tan enorme, lo que Anonymous ha proporcionado es una plataforma flexible para que los ciudadanos expresen su desacuerdo con las tendencias arraigadas desde hace mucho tiempo.

Pero BR1CKSQU4D, vinculada principalmente a la sensibilidad de sombrero negro, acabó su diatriba con una serie de amenazas que remitían directamente a la postura original de AntiSec:

> Si mostráis cualquier tipo de apoyo a antisec os convertiréis en un objetivo.
>
> Periodistas, músicos, abogados, servicios de alojamiento de web, proveedores de VPN, comentaristas políticos, empresas especuladoras, todos vosotros sois objetivos válidos.

Vosotros entrasteis en NUESTRO mundo; si no queréis participar en el juego, marchaos del puto campo de juego.

[...]

Amamos el espectáculo. Que se jodan los medios.

—BR1CKSQU4D

Capítulo 10

El deseo de un secreto es ser revelado

El verano en la ciudad de Nueva York es opresivo. Las elevadas temperaturas se combinan con la dura realidad metropolitana para crear un hellion* urbano distópico. Los rayos del sol, reflejados en los rascacielos de acero y cristal, te ciegan. Orificios subterráneos te llevan a las vísceras de la ciudad: los intestinos de las estaciones y las entrañas del sistema del metro que escupen gente hacia el exterior. Sudor, sonidos, vistas, como si todo esto no fuese suficiente: también estás cercado por la descomposición mefítica, con un olor similar al dorián, de la ciudad; olores a ratas muertas y detritus humanos horneados por las estaciones del metro. De modo que cuando, finalmente, se asienta el clima más fresco del otoño, la ciudad suspira con un alivio colectivo. Las hojas que cuelgan de las ramas de los árboles con una deslumbrante combinación de amarillo quemado, ámbar y anaranjado aportan un complemento a la tregua olfativa. El paso hacia el otoño se percibe como un nuevo aliciente en la vida. Finalmente, dejarás de sudar toda la noche. Finalmente, el hedor desaparecerá. Finalmente, un respiro.

El 17 de septiembre de 2011 me desperté junto a un ramillete de delicadas flores rosas, púrpuras y rojas que sobresalían de un florero encajado en una máscara de Guy Fawkes. Era mi cumpleaños. El momento era perfecto: un día de protesta en Nueva York. El colapso financiero había

grabado su marca de corrupción, oligarquía y el 1 por ciento en las mentes de una generación airada. En lugar de sentirme deprimida, oprimida e inmovilizada por la combinación de la situación financiera y el calor de la ciudad, el día era radiante y parecía haber un refrescante optimismo que la gente estaba dispuesta a aprovechar. Nadie quería llamarlo esperanza –era demasiado pronto para afirmar algo semejante— pero la posibilidad seguía encima de la mesa.

Agarré mi mascara y me dirigí a Bowling Green, cerca de Wall Street. Cuando me acercaba al pequeño parque cubierto de césped, con el rabillo del ojo vi a un grupo de jóvenes que llevaban máscaras de Guy Fawkes colgadas de los hombros. Al reparar en mi presencia, un par de ellos me saludaron asintiendo con la cabeza. Uno de ellos alzó el pulgar y me dijo «Sigue con tu buen trabajo». A primera hora de la tarde los manifestantes habían marchado hacia lo que se convirtió en el objetivo y centro neurálgico del acto, Zuccotti Park (rebautizado más tarde como Liberty Square). Muchos llegaban y se marchaban a medida que el día avanzaba hacia el crepúsculo y la primera Asamblea General, pero una corriente continua de jóvenes activistas continuaba llegando, acarreando material de acampada a la espalda que instalaban en el suelo.

Aun cuando Occupy Wall Street fue bautizado por asociación al lugar donde tuvo su arraigo, estaba claro que las redes sociales podían y debían desempeñar un papel vital en ese proceso. Sin ser *el agente*, ni siquiera *un agente* fundamental de la revolución, la comunicación virtual actuó más como un elemento adyuvante, aportó un impulso esencial, facilitó la coordinación y permitió que todos aquellos que no pudieron estar físicamente presentes presenciaran y se involucrasen en los acontecimientos. Y fue así que durante el primer día de Occupy, muchos de nosotros estuvimos enganchados a nuestros teléfonos móviles a pesar de estar presentes en la plaza. Aproximadamente cada media hora, buscaba el móvil en el bolsillo y consultaba los mensajes de Twitter. Por la tarde, dos mensajes consecutivos de Sabu aparecieron en la pantalla. Un mes antes, el 16 de agosto, Sabu había desaparecido de Twitter después de haber escrito enigmáticamente, «El mayor truco hecho jamás por el diablo fue convencer al mundo de que no existía. Y así... desaparece».[239] estos nuevos tuits señalaron su reaparición con un rugido:

«ATTN: nunca me marché, NO soy @AnonSabu ni ninguno de esos

posers. No he sido humillado, arrestado, hackeado ni ninguno de los demás rumores que circularon. Buscaros la vida.»[240] A este tuit le siguió otro: «Han intentado delatarme, trolearme, doxear a todos los que me rodean, me han provocado con argumentos interminables, pero hay una cosa que no pueden hacer: ¡FRENARME!»[241]

Durante una conversación de chat que mantuvimos a comienzos de agosto, Sabu me había avisado que iba a guardar silencio. «Sabu es un nombre que con el tiempo no será necesario que exista» fueron sus palabras.

<biella>: bien ok
<biella>: entonces :-/
<biella>: no estoy diciendo que sea sí ni tampoco que debes quedarte por aquí, solo digo que no desaparezcas Sabu
<Sabu>: bien
<Sabu>: no es que me marche para ser un gilipollas o para huir
<Sabu>: es solo que la propia comunidad
<Sabu>: necesita mirarse a sí misma para encontrar una motivación
<Sabu>: no a mí
<Sabu>: siento que me sigue demasiada gente
<Sabu>: y no estoy aquí para ser un líder. sí soy un líder nato
<Sabu>: y sí, si quisiera podría dirigir todo este movimiento sin la ayuda de nadie si quisiera vivir como un dictador
<Sabu>: pero la verdad es que
<Sabu>: no soy el líder de nada relacionado con anonymous
<Sabu>: y marchándome lo demuestro

Después de su salida de Twitter, y sin que yo lo supiera, Sabu continuó activo en varios canales secretos de IRC. También sin que yo lo supiera —y, en este caso, tampoco aquellos que trabajaban estrechamente con él online— el día anterior a nuestra conversación por chat, el 15 de agosto, había comparecido ante el tribunal. Sabu se había declarado culpable de los doce cargos presentados contra él, incluidos el de conspiración para cometer fraude bancario y robo de identidad con agravantes y tres cargos de conspiración para cometer hackeo informático. Enfrentado a 124 años de prisión, Sabu accedió a trabajar para el gobierno a cambio de una reducción de su sentencia máxima a cien años. También aceptó la «obligación de no

volver a cometer más delitos por ningún medio».[242]

A diferencia de su desaparición anterior en junio debido a su (también secreto) arresto, en esta ocasión había avisado a la gente que se iba a tomar un período de descanso. Los miembros de AntiSec iban y venían, un factor que contribuía a desactivar aún más las sospechas sobre Sabu. También creó una conexión permanente a IRC utilizando lo que habitualmente se conoce como un “bouncer de IRC” (programa que se utiliza para transmitir el tráfico y las conexiones en las redes de ordenadores), “proxy” o “sesión de pantalla”. Cuando él quisiera podía volver a unirse a la conexión permanente. Esto le permitía (a él y al FBI) tener acceso a todas las conversaciones mantenidas en los canales, y la gente podía enviarle mensajes incluso cuando no estaba conectado. El método utilizado por Sabu para conectarse no despertó ninguna sospecha porque es algo común entre los hackers, muchos de los cuales son adictos terminales, confiar en esos servidores proxy.

Cuando Sabu desapareció por primera vez, acepté su razonamiento al pie de la letra. Pero también había decidido ausentarse para desviar algunas acusaciones graves que hacía poco habían llegado a sus oídos. Justo antes de su desaparición pública en agosto, un hacker llamado Mike “Virus” Nieves acusó a Sabu de ser un chivato. Los registros de este intercambio aparecieron rápidamente en Pastebin. El asunto empezaba con Sabu sugiriendo indirectamente que alguien del equipo de Virus era un soplón. Virus contraatacó con fuerza:

<Virus>: en el caso de topiary, le delataste
<Virus>: es algo tan obvio sabu
<Sabu>: mi nigga [hombre negro con una cadena de oro en el cuello]
<Virus>: pero yo mantengo la boca cerrada
<Sabu>: será mejor que vigiles la puta boca porque no soy un soplón
<Virus>: yo no me meto
<Sabu>: y definitivamente no delaté a mi propio chico
<Virus>: no me importa si se infiltran en “Anonymous”
<Sabu>: puedo decirte exactamente cómo le arrestaron
<Virus>: nunca me gustaron, nunca me gustarán
<Sabu>: y si realmente supieras algo sabrías cómo le cogieron también
<Sabu>: durante un tiempo hubo un trol en twitter que se conectó a las menciones de topiary en twitter con

<Virus>: Anonymous no es más que un montón de perdedores gordos, llenos de granos, que viven en sótanos y se masturban más de 3 veces al día
<Sabu>: “jake de shetland”
<Sabu>: lo consiguió de unos foros de xbox
<Sabu>: topiary era un apasionado jugador de xbox
<Sabu>: era conocido en la comunidad hablaba mucho
<Sabu>: uno de los usuarios del foro le doxeó y siguió enviando la información ahí fuera
<Sabu>: bastaba que alguien fuese lo bastante inteligente para hacer la conexión
<Virus>: soy ingeniero social, ingeniero social profesional de hecho
<Sabu>: Yo también soy ingeniero social.[243]

Al principio, Sabu intentó negar la acusación cubriendo a Virus de elogios, pero cuando esa táctica fracasó, cambió de estrategia:

<Sabu>: deberías saber que si allanaran mi casa
<Sabu>: me entregaría
<Sabu>: soy del tipo mártir
<Sabu>: crecí en las calles
<Virus>: es una corazonada, nunca me equivoco
<Sabu>: esta vez te equivocas
<Sabu>: prefiero caer por mi propia mierda antes que delatar a mis propios niggas

En aquel momento las acusaciones parecía verosímiles, pero en modo alguno definitivas. Era igualmente probable que la disputa fuese consecuencia de un conflicto personal —un drama hacker— o que el propio Mike Virus fuese un soplón que estuviese tratando de llamar la atención. Virus reconoció incluso que había escasas pruebas para apoyar su acusación; confiaba en una corazonada. Como era habitual, Sabu se mostró amable *y* violento evitando las acusaciones.

En cualquier caso, el bajo perfil asumido por Sabu significaba que estaba siendo prudente. Durante su paréntesis, Anonymous hizo un buen trabajo. El grupo había ido a toda pastilla con OpBART y, poco tiempo después, Occupy concitó su atención colectiva. Hacer que una operación se desarrolle sin contratiempos requiere una creciente cantidad de comunicación y tiempo compartido en línea, de modo que no debe extrañar que en estos intensos momentos los rumores estallaran como una explosión de gases de humo o que se extinguieran tan abruptamente como habían

brotado. El regreso de Sabu el 17 de septiembre, el día que comenzó Occupy, fue un gesto astuto que contribuyó a alimentar su mito como un revolucionario auténtico. Al igual que un salmón que sabe regresar nadando miles de kilómetros río arriba hasta llegar al lugar donde nació, Sabu parece programado para hacer su aparición durante un importante acontecimiento político. Su reaparición envió el siguiente mensaje: «el atractivo de una protesta anula todo lo demás». Lo importante era la revolución. Y las acusaciones que parecían justificadas por su desaparición adquirieron rápidamente la apariencia de un drama sin fundamento.

Sabu parecía realmente entusiasmado con Occupy y, a medida que el movimiento adquiría impulso, enviaba mensajes frecuentes a través de Twitter. Otros Anons estaban igualmente preocupados. La concurrencia el primer día fue tan pobre que Nathan Schneider, que se convertiría en uno de los cronistas más prominentes del movimiento y más tarde escribió un libro sobre el mismo, recordó: «No pensé que duraría. No pensé que fuese a cambiar nada.»[244] Pero gracias a la persistencia de los ocupantes, gracias a los mensajes transmitidos a través de las redes sociales y gracias a la policía (que provocó la atención de los medios de comunicación y la indignación pública por cargar contra unos manifestantes y unas marchas pacíficos), en menos de dos semanas, Occupy pasó de unas brasas humeantes a una auténtica hoguera.

«TENGO LOS DÍAS CONTADOS»

La primera semana de Occupy regresé varias veces a la acampada— y más tarde me uniría a algunas de las numerosas marchas realizadas en Nueva York— pero como profesora a tiempo completo con dos clases, un libro por terminar y un programa de citas preparatorias de mi próxima mudanza a otro país, me resultaba difícil estar allí todo el tiempo que quería. En ocasiones, otros factores también me mantuvieron alejada de allí. El martes 20 de septiembre el día se me presentaba milagrosamente libre, pero al ver por la ventana que llovía, preferí contemplar otras maneras útiles de emplear mi tiempo. Y tal vez fue el destino, pero de no haber sido por esa perezosa reticencia tal vez nunca habría conocido a Sabu en persona. Por supuesto, al reflexionar ahora sobre cómo se desarrollaron los

acontecimientos, solo se me ocurre pensar que quizás habría sido mejor desafiar a la lluvia.

Aquel día, a última hora de la tarde y cuando ya había dejado de llover, me dirigí al NYSEC, el encuentro informal de los profesionales en seguridad. Fui caminando hasta el *Swift*, un bar en Greenwich Village. Desde la distancia divisé a weev, el famoso trol que había encabezado la operación Goatse Security y ahora vivía en la zona triestatal (Nueva York, Nueva Jersey y Connecticut) en espera de juicio. Llevaba un cigarrillo colgando de los labios y estaba hablando con dos personas que yo no conocía.

Weev estaba achispado y alegre. Se notaba que estaba calentando motores para lanzar una buena diatriba. Llevaba un pin de la Trinity Church, a cuyos servicios religiosos solía asistir, y el sermón que preparaba tenía como tema a Occupy. No estaba claro si apoyaba a Occupy o simplemente consideraba el movimiento una oportunidad para el troleo. Dio una charla memorable, ingeniándoselas para acusar a los malvados financieros, hacer referencia a la brutalidad policial mencionando a Oscar Grant, y hablar de las amenazas estatales contra los fabricantes de quesos artesanales, todo eso en apenas cuatro minutos. Pero en otros momentos weev también sostuvo una pancarta que decía «LOS CERDOS SIONISTAS NOS ROBAN A TODOS».[245] Weev me saludó. Al escuchar mi nombre, otro de los hackers arqueó las cejas. «¿Tú eres la Gabriella que estudia a Anonymous?», preguntó. Se lo confirmé. Weev nos puso al corriente de Occupy y entramos en el bar. Pedimos unas bebidas y nos instalamos en la sala trasera con los aproximadamente veinte hackers que ya estaban allí. Imaginé que el otro hacker (llamémosle Freddy) probablemente seguía a Anonymous a distancia, como muchos investigadores especializados en temas de seguridad, pero resultó que sabía mucho más de lo que yo podría haber imaginado. A medida que avanzaba la noche, Freddy y yo nos encontramos en un rincón oscuro del bar. «¿Eres agente del FBI?», preguntó, una pregunta que ya no me inquietaba como hacía unos meses atrás. Le contesté en un tono bastante molesto, «No. De hecho acabo de aceptar un puesto en Canadá. ¿Por qué me iba a enviar el FBI a un país al que generalmente ignoran, si trabajara para ellos?»

Estaba claro que tenía amplios conocimientos sobre Anonymous, incluso sobre los grupos que participaban en canales secretos de IRC como

#internetfeds. También me informó de que estaba organizando un encuentro entre Sabu y Parmy Olson, que estaba en proceso de escribir un libro sobre Anonymous. (Olson dice que esto en realidad no ocurrió, aunque reconoció haber estado en contacto con Freddy). Mientras se desarrollaba la conversación algo empezó a ser cada vez más evidente: estaba profundamente instalado en Anonymous y al parecer conocía a Sabu desde hacía bastante tiempo.

Freddy también dio a entender que Sabu estaba en Nueva York. Este dato coincidía con algunos indicios que había recibido directamente de él en nuestros chats. Pero cada vez circulaban más rumores sobre Sabu, muchos de los cuales afirmaban obstinadamente que vivía en Brasil. Era una posibilidad igualmente verosímil; Sabu trabajaba estrechamente con hackers brasileños y en Twitter se expresaba a menudo en portugués.

La información fluía en ambos sentidos: hice referencia a numerosos canales secretos de IRC frecuentados por AntiSec y AnonOps y compartí detalles de muchas "operaciones clandestinas". Esa información despertó su interés. Y entonces mencioné que me había criado en Puerto Rico. Al escuchar esto me ofreció a bocajarro: «¿Quieres conocer a Sabu?» Él podía organizarlo. Me quedé totalmente sorprendida. «Tengo curiosidad por conocerle, pero, francamente, soy escéptica.»

La conversación me ilusionó, no tanto por la perspectiva de conocer a Sabu —mi escepticismo era real— como por el placer que muchos hackers experimentan todo el tiempo: la utilización de secretos como un valioso objeto de intercambio. Los que escriben acerca del secretismo relatan habitualmente cómo un buscador de información puede, mediante la aportación de un secreto propio, inducir una revelación mayor por parte de su interlocutor. Graham Jones, un antropólogo que estudia los magos, describe el intercambio de secretos como «un símbolo de reconocimiento, un gesto de inclusión, un microrritual de iniciación y un movimiento en un sistema de intercambio».[246] Compartir secretos puede hacerse por venganza o para forjar la confianza. Puede tratarse de una simple exhibición de estatus o de una revelación calculada con la esperanza de provocar una respuesta. Pero cualesquiera que sean las razones y los mecanismos, a menudo los secretos compartidos engendran más secretos.

De regreso en el bar, mi cabeza era un torbellino. *¿Este es un tío normal o trabaja para el gobierno? Nos hemos conocido por casualidad...*

¿verdad? Finalmente decidí marcharme del bar. Una vez en casa, exhausta, transcribí cada detalle que era capaz de recordar antes de caer rendida y completamente vestida.

A la mañana siguiente, temprano, fui como de costumbre a un café del barrio. Un par de horas después estaba totalmente concentrada en mi trabajo mientras tomaba mi segundo o tercer café. Mi cliente en IRC, como era habitual, estaba conectado pero ignorado. Mi nombre destelló en la pantalla indicando que tenía un mensaje privado. Sumergida en modo trabajo, y sin permitir que nada me interrumpiese, atendí la consulta cuarenta minutos más tarde. Cambié de ventana:

<Sabu>: ¿estás?
<Sabu>: hola
<Sabu>: ¿estás ahí?
<biella>: hola
<biella>: sí
<biella>: estoy aquí
[...]
<Sabu>: comprueba tu puto buzón de voz loca
[...]
<biella>: lol me pregunto, ¿debería estar haciendo esto? :-)
<biella>: ¿darle mi número de teléfono móvil a uno de los hackers más famosos de todos los tiempos?
<biella>: deja que antes escuche mi buzón de voz pero sabes que alguien que conoces lo tiene
<biella>: ¿si fuera ahora a la oficina podrías hablar? ¿o solo debería escuchar mi buzón de voz?
<biella>: estoy al otro lado de la calle en una cafetería
<Sabu>: coño biella ve a escuchar el mensaje y luego bórralo

De regreso en mi oficina encontré un mensaje y un número. Llamé y nuestra primera conversación telefónica se prolongó durante una hora. Declarándose con arrogancia “el hacker más fiable”, preguntó, «¿Qué coño está pasando con los chivatos?» Luego continuó con una tipología dividida en tres partes: en primer lugar están los “infiltrados”. En segundo lugar están “los que buscan la fama”. Y, en tercer lugar, están “aquellos que están clavados a la pared y no quieren ir a la cárcel”. Casi todo lo que decía hizo que perdiera de vista al propio Sabu. Pero, por si albergaba alguna duda,

insistió con declaraciones como: «Incluso si el FBI estuviese al otro lado de la puerta y escuchara lo que he dicho, no hay manera de que pudieran colgarme técnicamente el hecho a mí... Por eso no estoy encarcelado.» En aquel momento me pareció una explicación absolutamente plausible.

El resto de la conversación se centró sobre todo en cuestiones políticas, con Sabu despotricando y alardeando y yo escuchando. Arremetió contra el Departamento de Policía de Nueva York, afirmando que eran mucho más corruptos que el FBI, dispuestos a plantar información falsa y vulnerar sus propias reglas. Criticó a Sony y AT&T, insistiendo en que *ellos* eran los delincuentes por el desastroso estado de su seguridad. La conversación incluyó luego a WikiLeaks. Sabu afirmó que era una “tragedia” que Assange hubiera desaprovechado una magnífica oportunidad, pero finalmente expresó su amor por Manning.

Al final no tuve más remedio que interrumpirle y preguntar «¿Por qué salir a la luz?»

Su respuesta fue instantánea. «Tengo los días contados –explicó—. Esta historia necesita conocerse y los medios de comunicación no están por la labor.» La conversación terminó y me dejó reflexionando sobre qué había querido decir exactamente con eso.

No pasó mucho tiempo antes de que volviésemos a hablar. Esta vez Sabu estaba en la calle, algo que resultaba evidente por las bocinas de los coches y las conversaciones marginales entre sus colegas y él. Me dijo, «los polis están persiguiendo a un chico negro por una bolsa de hierba». Esta segunda conversación se centró en su defensa del estilo de hackeo practicado por Anonymous. «No somos ningunos skids», insistió, aludiendo con ese término a los eternamente ridiculizados “script kiddies”. Luego describió a LulzSec como una “prueba de concepto” que había hecho «más que cualquier otro grupo de hackers en los últimos quince años». Dijo que AntiSec era su creación.

Yo estaba escribiendo a una velocidad vertiginosa pero, no acostumbrada a tomar notas a mano, mi agarrotada muñeca demostró no estar a la altura de la tarea exigida. Al final nada de todo eso resultó demasiado sorprendente. Es decir, hasta que llegamos a la parte final de la conversación. «Espero no sonar como un gilipollas —comenzó diciendo—. Pero me niego a permitir que mi política muera. Así es como lo siento. Continuaré insistiendo en la idea de la organización descentralizada.» Hizo

una pausa antes de continuar: «Con la descentralización resulta más difícil infiltrarse.» Pero, «hay chivatos». Acabó bruscamente. Quería guerra. «Quiero una venganza total por Recursion. No es más que un estudiante universitario.» Hacía apenas unos días, Cody Kretsinger, cuyo apodo era Recursion, un joven de 23 años de Phoenix, Arizona, había sido arrestado por el FBI en relación con el hackeo de Sony Pictures con LulzSec.

Durante estas primeras conversaciones telefónicas, Sabu había sugerido que quería que nos conociéramos. Yo estaba cada vez más interesada en esa posibilidad pero también estaba decidida a no quedarme esperando a que me llamara. Mientras tanto había mucho que hacer, a medida que aumentaba la implicación de Anonymous en Occupy. Mientras se sucedían las acampadas por toda América del Norte y Europa, un puñado de sólidos veteranos de Anonymous cambiaron días y noches online por días y noches sobre el terreno. Algunos de ellos hasta encontraron a contingentes de ocupantes a quienes identificaron como Anons pero que nunca se habían conectado a un canal de IRC.

En ocasiones los dos movimientos, diferentes aunque complementarios, cruzaron directamente sus caminos de un modo más espectacular. El domingo 25 de septiembre, los manifestantes se reunieron en Union Square e iniciaron una marcha hacia el sur en dirección a la acampada, hasta que la policía los encerró detrás de una malla de plástico anaranjado. Los ocupantes comenzaron a corear, «¡Vergüenza! ¡Vergüenza! ¡¿A quién estáis protegiendo?! VOSOTROS sois el 99 por ciento! ¡Estáis combatiendo a vuestra propia gente!» Un agente de policía de alto rango, Anthony Bologna, sacó su bote de spray de pimienta sin que mediara ninguna provocación y dirigió el chorro químico contra tres mujeres jóvenes. Cuando el líquido impactó en sus rostros y comenzó a escocerles los ojos cayeron al suelo encogidas y suplicando, «¡No! ¿Por qué lo hace?!»[247] La respuesta de Bologna fue alejarse de allí caminando tranquilamente.

Los espectadores grabaron todo el incidente y el vídeo se viralizó. Anonymous tomó represalias doxeando rápidamente al policía, subiendo su nombre y dirección a Pastebin. Comenzaba con este mensaje:

> Mientras estábamos mirando, un agente roció a mujeres inocentes, vimos el salvaje spray de pimienta dirigido violentamente contra un

> grupo de mujeres. Nos quedamos conmocionados y asqueados por su conducta. Tú sabes quiénes eran esas mujeres inocentes, ahora ellas podrán saber quién eres tú. Antes de volver a cometer una atrocidad contra personas inocentes, piénsatelo dos veces. ¡ESTAMOS VIGILANDO!!! ¡Espéranos![248]

La información sobre Bologna fue subida a la red por una joven estudiante universitaria que se "ganó sus galones" en el CabinCr3w por su esfuerzo. Durante una entrevista online que mantuve con ella me explicó la mecánica de su exposición: «Miré mil veces [el vídeo], acercando la imagen con el zoom, tratando de captar sus rasgos faciales, el número de la placa y un nombre parcial. Resultó que cuando recurrí a una simple búsqueda en Google descubrí que el tío ya había tenido anteriormente problemas de abuso policial y que tenía una causa abierta contra él.» (Una demanda pendiente contra Bologna presentada por un manifestante durante la celebración de la Convención Nacional del Partido Republicano en Nueva York en 2004.)

Puesto que no me pareció que fuera alguien que se dedicaba a doxear en la red por amor al arte, le pregunté dónde trazaba ella la línea entre la divulgación aceptable de datos y la violación de la privacidad: «[la policía] trabaja para el público, por lo tanto tu vida... es pública igual que te tratarían los medios de comunicación que te acosaran.» Y prosiguió, «en términos morales: creo que hay un límite y una barrera que determina la profundidad que debe alcanzar el doxeo», afirmando que ella solo divulgó información que identificaba al propio Bologna. Otros Anons, sin embargo, decidieron ir aún más lejos, doxeando a miembros de su familia.

Al principio, el Departamento de Policía de Nueva York defendió las acciones de Bologna, pero pronto se retractó. Una investigación interna de la policía determinó que el oficial había violado efectivamente el protocolo. Como castigo perdió diez días de vacaciones y fue reasignado a Staten Island (revelando de manera implícita la opinión que tenía el Departamento de Policía de Nueva York del distrito más pequeño de la ciudad).[249] Hubo, al menos, un aspecto positivo. El incidente contribuyó a catapultar a Occupy a la escena nacional. *The Guardian* y otros importantes medios de comunicación informaron acerca de este hecho, citando directamente el mensaje de Anonymous en Pastebin y consolidando una incipiente

asociación entre Anonymous y Occupy.[250] A partir de aquel día —y sobre todo después de que se produjera el arresto masivo de más de setecientas personas durante la celebración de una marcha pacífica por el puente de Brooklyn— Occupy se convirtió en un elemento permanente tanto en los círculos activistas como en los principales medios de comunicación.

Encuentro con Sabu

Gracias a detalladas y frecuentes preguntas publicadas por el Departamento de Servicios de Informática y Telecomunicaciones de Nueva York sabemos aproximadamente cuántos teléfonos públicos hay en los cinco distritos: «El 2 de enero de 2014 hay 9.903 teléfonos públicos activos en las aceras de la ciudad o junto a ellas.»[251] Yo, personalmente, ni siquiera había reparado nunca en ellos hasta que Sabu me pidió que utilizara uno. No quería concretar un encuentro por la red. Era más seguro y prudente utilizar un teléfono público; con los ordenadores siempre cabe la posibilidad de que haya generadores de claves.

Nuestra primera cita quedó programada para poco después que se produjera el doxeo a Bologna, el 3 de octubre, en el *Chipotle* de St. Mark's Place, en el East Village. Sabu me aseguró que "me reconocerás". La única fotografía que figuraba ser de Sabu que circulaba por la red era la de un tío latino delgado pero musculoso. Llegué temprano al lugar de la cita. Los minutos avanzaron lentamente hasta que, de pronto, me di cuenta de que una figura alta e imponente se acercaba a mí. Llevando su cuerpo grande con evidente aplomo, parecía encontrarse en su elemento. Era Sabu. Me cogió la mano y temí que me la aplastara. Cogí mis cosas y fuimos a buscar algo de comer. En medio de nuestra conversación superficial, Sabu hizo una pausa, saludó con la cabeza a la chica que preparaba la comida (una chica latina de aspecto duro), y le preguntó, «¿Qué hay?»

Ella contestó, «hace tiempo que no te veía por aquí». Como resultaría cada vez más claro, ya fuese en *Chipotle*, un restaurante local, o en el Tompkins Square Park, mucha gente conocía a Sabu y le trataba con deferencia. No podría decir si era por respeto o por temor, pero era evidente que se trataba de un personaje conocido en el vecindario.

Poco después, Sabu dirigió la conversación hacia su pasado. «Vengo

de una familia de traficantes de droga —reveló casi de inmediato, antes de continuar con tono despreocupado—: A los trece o catorce años ya llevaba entre cuatro y cinco mil dólares en la cartera.» También me explicó que era la “figura paterna” para sus primas adoptivas —ambas menores de siete años en aquel momento— aunque no mencionó hasta bastante después la razón que le llevó a asumir esas enormes responsabilidades parentales. (Cuando Sabu tenía trece años, su tía y su padre fueron enviados a la cárcel por traficar con heroína. Fue criado por su abuela hasta que ella murió el ٧ de junio de ٢٠١٠, exactamente un año antes de que le detuviera el FBI. Después de la muerte de su abuela, él asumió la responsabilidad parental de sus primas.)

Sabu dijo que había trabajado duro para superar la “mentalidad de gueto”, una mezcla paralizante de ira y odio hacia sí mismo. Más tarde refirió brevemente algunos episodios que corroboraban su experiencia cotidiana con el racismo puro y duro. Sabu había asistido a la Washington Irving High School, cerca de la Calle 16 Este, junto a muchos estudiantes pobres. Un día, cuando entraba en la escuela, pasó a través de un detector de metales y, como llevaba encima un destornillador, un guardia le detuvo. Él se defendió: «Soy el geek que arregla el sistema cuando ustedes se olvidan de que no deben ejecutar archivos exe ‘raros.» El guardia no se tragó la historia y se produjo una discusión acalorada entre ambos. Sabu, que se sentía menospreciado, se quejó a la dirección del centro, pero nadie le hizo caso. De modo que decidió hacer un poco de ruido redactando una carta incisiva y supuestamente “controvertida” y la hizo circular entre los profesores. El director consideró que el escrito era “amenazador” y Sabu fue expulsado temporalmente. Al reflexionar más tarde sobre ese incidente en un documento colgado en Pastebin, llegó a la siguiente conclusión: «Muy bien entonces, es una vergüenza tan grande que a alguien... como yo se le privara de su educación debido a algo que había escrito.»[252]

Tuvo sentido de inmediato, entonces, que Sabu hubiera encontrado en el hackeo —con su elevado nivel de argumentos e ideas—un oasis muy atractivo. Esto no significa decir que el ámbito del hackeo esté libre de prejuicios. En absoluto. El panorama, dominado por el hombre blanco, algunos de ellos especialmente proclives a representar la figura del pistolero elitista, resulta alienante y repugnante para muchos.[253] Las barreras son especialmente pronunciadas en los sectores underground que están

compuestos casi exclusivamente de participantes masculinos (y unos pocos transgénero). No obstante, puesto que las ideas son (en teoría) glorificadas por encima del pedigrí social, ha funcionado como un espacio seguro, al menos online, para una clase de bichos raros tecnológicos.[254] Los límites sociales establecidos por los hackers también muestran contradicciones: aunque la brecha del género es enorme, algunas identidades —tales como transexual, homosexual o discapacitado— son más comunes y aceptadas. (Me llevó algún tiempo, pero finalmente descubrí que la sala de chat #lounge en AnonOps en ocasiones hacía las veces de sitio de ligue para gays.) La explicación de Sabu de que él «raramente hace vida social con hackers» apunta a la clase de libertades parciales que proporcionan el anonimato y las habilidades técnicas online.

Una vez que nos despedimos, no pude evitar pensar en Sabu como en una versión más guay e inteligente de Oscar Wao, el personaje principal de la electrizante novela de Junot Díaz sobre los problemas de ser un nerd corpulento, marginado, descendiente de dominicanos y amante de la "fantasía y la ciencia ficción dura". *La maravillosa vida breve de Óscar Wao* (Mondadori, 2008*)* cuenta la historia de Óscar mientras viaja entre Nueva Jersey y la República Dominicana, avanzando trabajosamente por la vida mientras intenta cumplir un anhelado rito de iniciación: acostarse con una mujer.

Sabu, al igual que Óscar, es un consumado "cruzador de fronteras culturales", saltando con facilidad entre esferas culturales enormemente diferentes. A diferencia de Óscar, Sabu no era ningún estúpido y su machismo resultaba abrumador. Era famoso por intentar ligarse a las mujeres en #AnonOps y en una conversación de chat le dijo a la periodista Quinn Norton, «Me gustas quinn, la próxima vez que estés en nueva york, puedes mirarme cuando hackeo, desnudo».[255] Conmigo se mostró más contenido, alternando entre llamarme "mi amor" [en español en el original] y "bombón".

Después de nuestro primer encuentro, ahora equipada mentalmente con una imagen de Sabu, reanudé mis chats con él. El periódico *The Guardian* le había pedido que escribiese un artículo sobre Occupy. Sabu me pidió que le diese algo de información editorial. Mientras tanto, yo intentaba convencerle de que apareciera en el documental de Brian Knappenberger *Somos legión*:

<Sabu>: además
<Sabu>: si haces esta cosa con tu chico knapp
<Sabu>: tienes que asegurarte de que ese nigga no filtra mi identidad

Más que cualquier otro periodista que abordara el tema de Anonymous, Brian Knappenberger había buscado una amplia muestra representativa de individuos, invirtiendo su tiempo y su dinero en un proyecto por el que sentía auténtica pasión. Yo quería ayudarle. El hecho de que Sabu estuviese considerando la posibilidad de participar en ese proyecto era una gran noticia, pero tuve que darle nuevas pruebas de mi capacidad para ser discreta y de hacer entender a Knappenberger la necesidad de una absoluta discreción. En general mi protocolo era uno de “silos de interacción”. Cuando chateaba en los canales públicos, un observador podía hacerse una idea de con quién estaba hablando, pero mis chats privados eran básicamente confidenciales y seguían un protocolo habitual adoptado en Anonymous. Finalmente, un pequeño grupo de la confederación de periodistas/investigadores —principalmente Knappenberger y Olson— supo que había conocido a Sabu pero, por lo demás, me guardé esa información para mí.

Al analizarlas retrospectivamente, en ocasiones nuestras conversaciones en apariencia triviales se volvían mucho más interesantes. Por ejemplo, la siguiente conversación, que mantuvimos el día después de habernos conocido, en su momento me pareció relativamente banal:

<Sabu>: y ioerror es buena gente [ioerror = el desarrollador de Tor Jacob Appelbaum]
<Sabu>: estoy tratando de ponerme en contacto con él
<Sabu>: sé que ha sido solidario conmigo el año pasado
<Sabu>: y quiero ser solidario con él
<biella>: así es
<Sabu>: durante este tiempo
<biella>: le conozco bien
<Sabu>: están tratando de obligarle a que hable
<biella>: desde hace más de ٩ años
<Sabu>: dile que le envío recuerdos
<biella>: lo haré seguro
<Sabu>: si hay algo que nosotros podamos hacer por él, que lo pase a través de ti

En aquel momento lo interpreté como un gesto razonable de solidaridad. Hoy estos chats —y sus motivos para ponerse en contacto conmigo en primer lugar— tienen un significado muy distinto. El “nosotros” al que se refería no era Sabu y Anonymous. Era Sabu y el FBI, privilegiado con acceso directo a todas sus conversaciones, incluida la descrita más arriba. No sería la última vez que Sabu intentaría “ponerse en contacto” con Applebaum a través de mí.

La propensión a comprender a los demás

A finales de octubre, cuando los vientos agitaban las hojas que aún colgaban de las ramas, Occupy estaba floreciendo. Los organizadores se diversificaban; las alianzas forjadas con los sindicatos y otros grupos de la sociedad civil generaban nuevos ríos de gente que fluían hacia Liberty Square el 15 de octubre, un “Día Mundial de Acción” perfectamente planificado. Mientras yo marchaba durante horas junto a una multitud de desconocidos, todo el mundo parecía estar lleno de energía y maravillado por el giro dinámico que había tomado Occupy en el breve lapso de un mes. «Las asambleas de Occupy estaban abriendo un enorme espacio en el discurso político estadounidense», reflexionó Nathan Schneider, quien también señaló que «hacia mediados de octubre, el movimiento Occupy Wall Street tenía un índice de aprobación superior al 50 por ciento, más alto que el presidente Obama o el Congreso».[256]

Los detractores y entendidos acusaban a Occupy de estar dirigido por activistas sobre cómo hay que vivir la vida, de esfumarse después de haber sido incapaz de movilizar un amplio apoyo de las bases; un relato equivocado que quedó patente con la campaña represiva que se produciría apenas un mes más tarde para erradicar muchas de las acampadas organizadas en Estados Unidos. Los documentos obtenidos por la Partnership for Civil Justice Fund mediante la apelación a la Ley de Libertad de Información revela que prácticamente todas la entidades del orden público —el Departamento de Seguridad Nacional, el FBI, la policía local, los Fusion Centers (centros regionales conjuntos para la integración de información), las Fuerzas Especiales Conjuntas contra el Terrorismo, el Servicio de Investigación Criminal Naval e incluso, curiosamente, la

Reserva Federal— demostraron un gran interés por Occupy.[257] Puesto que los textos de los documentos están notablemente censurados resulta muy difícil determinar la función específica que cumplía cada organización, pero es evidente que, como mínimo, «lanzan [una] amplia red para vigilar las protestas de Occupy», como tituló *The New York Times* el artículo que hacía referencia a estos documentos.[258] Una de las razones por las que Anonymous había prosperado durante cinco años era que, a pesar de los arrestos sufridos por miembros del colectivo, su carácter descentralizado y online había convertido la prevención en una tarea extremadamente complicada. No sería el caso de Occupy.

Yo continuaba reuniéndome con Sabu. En algunas ocasiones le acompañaban sus dos hermanos menores. El mayor era el escudero de Sabu. Le admiraba y, aunque técnicamente no era tan competente como él, le encantaba hablar de ordenadores. El más pequeño, que lucía una mata de pelo lisa y brillante, negra como el ala de un cuervo, y un montón de músculos, estaba, como muchos adolescentes, sumido en sus pensamientos, absolutamente indiferente a la conversación de geeks que manteníamos el resto de nosotros.

Uno de esos encuentros se destaca por encima de los demás. Una tarde de noviembre inusualmente calurosa dimos un paseo por Tompkins Square Park de nuevo acompañados por sus hermanos. Luego Sabu y yo fuimos a *The Odessa*, un restaurante clásico de Nueva York que tiene una variedad de platos realmente alucinante. Para entonces una cosa había quedado clara: Sabu era muy parlanchín. Al entrar en el local, Sabu saludó con un apretón de manos a un tipo que supuse que era el dueño o el gerente del lugar. Una vez instalados en uno de los reservados nos fundimos con los añejos asientos de vinilo, sus trajinados muelles aferrándose a nosotros desesperadamente. Aquel día Sabu abordó una abrumadora cantidad de temas en el curso de nuestra conversación: el aburguesamiento de algunos barrios, el hacker Phiber Optik, la política en Oriente Medio, Occupy, su perro (cuyo nombre era *China* y sufría una horrible enfermedad en la piel), la sociología de los grupos hacker, los que odiaban a Anonymous y docenas de otras cuestiones que le pasaban por la cabeza. Entre todo aquel diluvio de detalles, un par de ellos sobresalió del resto. Era la primera vez que mencionaba a un misterioso hacker con quien trabajaba estrechamente y a quien llamaba “burn”. Yo le conozco como Jeremy Hammond. Sabu

presumía de que a él le gustaba hackear a empresas de seguridad mientras que «a burn le gustaba atacar a la policía». Y en esta conversación una cosa quedó patente: más que cualquier otra cosa, a Sabu parecía preocuparle realmente lo que los demás pensaban no solo de él, sino de Anonymous en su conjunto. Su desprecio hacia los críticos de Anonymous —tanto periodistas como la gente en Twitter— era notable; se mofaba de aquellos que pensaba que no le habían tratado a él, o a Anonymous, con respeto. Poco después, al acabar su discurso, suspiró con voz cansada. «A veces solo me apetece largarme y dejarlo todo.» Parecía realmente cansado y desde nuestro último encuentro había desarrollado una tos crónica. Yo sabía también que había hablado extensamente con Olson a través de Skype, y de pronto tuve la sensación de que le consumía un deseo ardiente de que el mundo conociera su historia.

Cuando alguien lleva una máscara existe al menos un recordatorio simbólico de que la falta de sinceridad, la duplicidad y el juego podrían estar actuando. Sentada frente a Sabu, mientras observaba su expresión, escuchaba su voz y le miraba a los ojos, dejé de lado mi desconfianza, aun cuando sabía que, con o sin máscara, yo no tenía realmente acceso a sus verdaderas motivaciones. Nunca podemos tener realmente acceso a los pensamientos íntimos de otros seres humanos; solo podemos intentar determinar su sinceridad o autenticidad. Luego está lo que Hume identificó como una de las cualidades más perdurables de la naturaleza humana: «Ninguna cualidad de la naturaleza humana es tan destacable, tanto en sí misma como en sus consecuencias, como la propensión a comprender a los demás.»[259]

Es difícil cuestionar permanentemente los motivos que animan a la gente. Es precisamente la proclividad humana a desear comprender a los otros lo que permite que el FBI lleve a cabo exploits a través de sus informantes. Nos marchamos de *The Odessa* y, como de costumbre, Sabu encendió un cigarrillo perfumado. Dio una profunda calada desde el filtro blanco. Y luego, súbitamente, confesó: «Yo era efectivamente un delincuente. Solía vender heroína.» Luego se alejó.

Capítulo 11

El Sabutaje

Si bien AntiSec se había dedicado a la juerga del hackeo, poniendo en peligro a objetivos de alto nivel como el FBI, el grupo no estaba recibiendo demasiada atención, y la que recibía no era precisamente positiva. Algunos vaciados de memoria, como los que afectaban a las unidades de la policía (incluidos la Asociación Internacional de Jefes de Policía, la Asociación de Patrulleros de la Policía de Boston y la Oficina del Sheriff del Condado de Baldwin, en Alabama) impactaron a algunos Anons por arbitrarios e incoherentes. Muchas personas, incluso dentro del colectivo de Anonymous, directamente no entendían cuál era el objetivo de esas acciones. Uno de los partidarios de las filtraciones de información, Anonymous9, opinaba que las operaciones llevadas a cabo por AntiSec no estaban a la altura de las expectativas creadas. «El simple hecho que un menú de mediodía en Fort Meade pueda ser material secreto —me explicó — no significa que sea interesante, ni mucho menos que merezca ser filtrado.» Entonces, justo a tiempo para el “LulzXmas”, un misterioso hacker llamado hyrriiya envío un regalo. El 13 de diciembre de 2011, unos cuantos miembros de AntiSec nos llevaron aparte a la periodista Quinn Norton y a mí a un canal privado para hacernos una pregunta:

<Antisec>: cubrirán los periodistas un asunto que probablemente sea
<Antisec>: profundamente ilegal
<Antisec>: lol
<quinn>: si, pero el contexto es importante
<Antisec2>: No ilegal como el doseo o filtrar los correos electrónicos de unos polis. ;)

<biella>: profundamente, como opuesto a superficialmente, ilegal
<Anon>: tenemos una tabla de categorías ilegales
[...]
***Anon comprueba la hoja de referencia
<biella>: Anon, ¿de verdad??
<biella>: lol
***Anon piensa 'mierda estamos jodidos'
<quinn>: ¿es como una especie de tabla de mínimos obligatorios?
<quinn>: jeje
<Anon>: jajaa
<biella>: LO QUE ESTÁ FUERA DE ESA TABLA es ilegal

Poco después de haber mantenido este chat, un miembro de AntiSec me informó que tenían en su poder datos de tarjetas de crédito y pretendían utilizarlos para hacer donaciones benéficas. Aunque mantuvo en secreto la fuente de esa base de datos, sigue siendo una de las escasas ocasiones en las que me revelaron información sensible. Yo mantuve públicamente mi advertencia: no podía garantizar la confidencialidad de ninguna información que ellos me proporcionaran. Y, como si eso no bastara para inquietarme, el 15 de diciembre Jeremy Hammond (utilizando el nombre "sup_g") me hizo una consulta:

<sup_g>: No estoy seguro de si estás interesada, si eres capaz o si estás segura de querer examinar un prelanzamiento de datos, pero hay disponible una cola de correos electrónicos.
<biella>: en este momento no, lo siento :-(aunque espero tener noticias de ese asunto

Para entonces mis interacciones con Hammond eran limitadas y contenidas. La mayoría de nuestras conversaciones se desarrollaba en chats grupales en el canal privado CabinCr3w (donde él era "sup_g") y en el Proyecto PM de Barrett Brown (donde él era "o"). Con el tiempo llegué a vincular estos dos apodos y no conseguía tomar una decisión con respecto a Hammond. Mantenía un perfil bastante discreto, excepto cuando las discusiones políticas le sacaban de las sombras y, de pronto, inundaba el chat con sus opiniones de una manera bastante acalorada. Hammond era sin duda alguna el miembro más insurgente del grupo. Aunque su dedicación era evidente, a veces no podía evitar pensar que se trataba de un agente provocador.

Cuando me ofreció examinar el prelanzamiento de esa cola de correos electrónicos, se dispararon todas mis alarmas. ¿Se trata de una trampa? A diferencia de Brown, cuyo deseo de hacerse con estos mismos correos electrónicos cayó en los oídos sordos de AntiSec (nunca se los entregaron), yo trataba desesperadamente de evitar que compartiesen conmigo esta clase de información. Y, en cualquier caso, ¿por qué —después de todas mis advertencias y todos sus intentos de permanecer en silencio— ofrecían de pronto lanzarme toda esta información? Me pareció un movimiento sospechoso y me provocó gran inquietud.

En realidad, por suerte, me mantenían al margen de un arsenal de secretos más profundo. Más significativo era que el grupo de AntiSec, a principios de diciembre, hubiera comenzado a albergar grandes sospechas respecto a Sabu. Según me explicó más tarde uno de sus miembros, continuaron apareciendo varios hackers, de forma aleatoria, para insistir, como si se tratase de un mantra, en que «Sabu es un informador». Hammond también se había cansado de la reticencia de Sabu a ensuciarse las manos, un claro indicador de que había algo que no cuadraba. En aquellos días se guardaron sus preocupaciones para ellos.

En Nochebuena, AntiSec decidió hacer públicos los detalles de su hackeo más memorable e implacable. En un acto de sabotaje corporativo con clara motivación política, AntiSec se infiltró en la red interna de la empresa de inteligencia global Strategic Forecasting, Inc., más conocida como Stratfor. Hackearon más de 50.000 números de tarjetas de crédito, descargaron casi ocho años de correos electrónicos de la empresa —cinco millones en total— y se hicieron con innumerables documentos de otra naturaleza. Como traca final destriparon los datos de los servidores de Stratfor, extrayendo todo lo que pudieron encontrar (incluidas las copias de seguridad). En lo que describieron como «un acto de amorosa delincuencia igualitaria»[260] intentaron utilizar 30.000 de esas tarjetas de crédito para donar alrededor de 700.000 dólares a la «organización de apoyo a Bradley Manning, la EFF (Electronic Frontier Foundation, una organización sin ánimo de lucro con sede en San Francisco que dedica sus esfuerzos a preservar los derechos de libertad de expresión), la ACLU (Unión Estadounidense de Defensa de las Libertades Civiles), CARE (una organización internacional dedicada a combatir la pobreza), la Cruz Roja Americana, Amnistía Internacional, Greenpeace, algunos comunistas,

algunos presos, diversos activistas y a muchos más colegas anónimos».[261] (Solo 9.561 de las tarjetas seguían siendo válidas.) Examinemos ahora más detenidamente los hechos que condujeron a la madre de todos los hackeos llevados a cabo por AntiSec.

Caos total

El 4 de diciembre, hyrriiya, miembro de un pequeño grupo de hackers llamado RevoluSec (que trabajó infiltrándose en los ordenadores del gobierno sirio, entre otros proyectos) se puso en contacto con Sabu:

> <hyrriiya>: despierta
> <hyrriiya>: tengo una mierda divertida que te encantará
> <Sabu>: estoy aquí hermano
> <Sabu>: qué pasa
> <hyrriiya>: :=
> <hyrriiya>: total que hackeé a esta empresa de inteligencia
> <hyrriiya>: por accidente

Esta información despertó de inmediato el interés de Sabu:

> <Sabu>: nos encantaría penetrar en sus usuarios/red porque #antisec definitivamente me consigue detalles para que pueda comenzar a a trabajar:)
> <hyrriiya>: :p [sacar la lengua en un gesto de sorpresa/admiración]
> <hyrriiya>: la red está en espera en este momento
> <hyrriiya>: tan pronto como extraiga lo que necesito
> <hyrriiya>: te lo entregaré
> <hyrriiya>: pero te aconsejaría que los controlaras y vigilaras durante unos meses
> <hyrriiya>: los servicios secretos de mis propios países emplean sus servicios:p
> <hyrriiya>: la cnn los emplea
> <hyrriiya>: etc
> <hyrriiya>: the economist lol

Al día siguiente hyrriiya proporcionó, según me contó Jeremy Hammond, «a todo el canal [de AntiSec] un enlace a las bases de datos de Stratfor, incluidos direcciones, y tarjetas de crédito [y] números de tarjetas de crédito obtenidas al azar de la base de datos de Stratfor». Sabu creó otro canal

llamado “#!sec” y hyrriiya facilitó la información relacionada con el exploit. Hammond me describió el hackeo con profusión de detalles técnicos (si bien no es un dato esencial para entender la historia):

> No hay contraseña, ¡uy! Lo que te permite descargar todo el registro de la base de datos, desde el acceso a la base de datos mysql puedo insertar a los usuarios en el sistema drupal de str’s [Stratfor’s], creando una cuenta de administrador predefinida, habilitando luego el código PHP en los artículos drupal e insertando una puerta trasera PHP en un artículo drupal que permite la ejecución remota de un código en el servidor de web de str’s (mantenían diferentes casillas para varios servicios), luego pude enrutar el servidor de web y conectarme a su servidor de correo utilizando un usuario “autobot” que tenía acceso a varios de sus otros servidores internos con finalidades de copias de seguridad y también lo enruté.

Como si carecer de la protección que ofrece una contraseña no fuese una negligencia suficiente, habían guardado la información de las tarjetas de crédito de Stratfor en formato de texto normal en lugar de hacerlo protegiéndola detrás de una fortaleza digital de encriptación, como es la práctica estándar en esta industria. Aparentemente, mientras Stratfor vendía a sus clientes sesiones informativas sobre seguridad, la empresa no parecía aplicar ninguno de sus propios consejos.

AntiSec pretendía liberar ocho años de correos electrónicos de los servidores de Stratfor’s, o sea, más de doscientos gigabytes. Encontrar un buen lugar donde colocarlo, con el suficiente espacio y ancho de banda, era un pequeño problema. Hammond optó por hackear algunas otras máquinas para prestar este servicio. Algunos otros miembros de AntiSec comenzaron a investigar métodos para realizar una infiltración más profunda en los sistemas de Stratfor, mientras que otros que solo habían querido iniciar el incendio no tardaron en marcharse.

Hyrriiya solo desempeñó un papel de mensajero y finalmente sacó de apuros el resto de la operación:

<hyrriiya>: también otra cosa
<hyrriiya>: cuando te consiga los detalles

<hyrriiya>: por favor olvida que fui yo quien te los dio :)
<hyrriiya>: y que revolusec tuvo nada que ver con esto :p
<hyrriiya>: porque esta compañía está llena de federales chiflados :p
<hyrriiya>: y no necesitamos el crédito.)
<hyrriiya>: :)
<Sabu>: de acuerdo
<Sabu>: #antisec lleva en guerra con los federales/la otan desde junio

En Nochebuena recibí una consulta de un misterioso usuario llamado “ghost__”, otra encarnación del propio Hammond, según supe más tarde. Me dio la noticia más explosiva que recibiría durante todo el tiempo en que estuve estudiando a Anonymous:

<ghost__>: hola
<ghost__>: la mierda se está apoderado de anonops
<biella>: hola
<ghost__>: a punto de rm -rf un objetivo importante

No estaba segura de a qué se refería con su primera declaración, pero la segunda estaba clara. Puede que no sea una maga de la tecnología, pero sabía lo que era “rm -rf/”, ya que hacía más de catorce años que utilizaba el sistema operativo Linux. Una vez que tienes acceso a servicios desde root, este comando puede borrar todo lo que contiene el sistema (técnicamente hablando, Hammond comunicó sus acciones taquigráficamente porque los nuevos sistemas UNIX llevan la protección incorporada, tal como solicitar que se apruebe primero el indicador “--no-preserve-root” haciendo que resulte más difícil borrarlo todo tecleando accidentalmente seis caracteres). Intenté tomármelo con calma. Aún no estaba segura de sobre qué me estaba hablando. Me dio unos cuantos detalles más:

<ghost__>: es una de las empresas de inteligencia más importantes
<ghost__>: ~30 min
<biella>: hmm ok
<ghost__>: mientras tanto, las tarjetas de crédito se están utilizando en anonops

Muy pronto mi confusión se disipó gracias a tuits como el siguiente enviado por Sabu: “http://www.stratfor.com - #ANTISEC DESMANTELA UNA CORPORACIÓN DE INTELIGENCIA MULTIMILLONARIA - mirar el

vídeo y leer el ensayo. #antisec.”[262] Pensé para mí, ¡por los clavos de Cristo, *está pasando realmente!*

Un puñado de gente estaba furiosa o confusa, pero la mayoría parecía estar surfeando la ola con respuestas trolísticas/humorísticas en los canales públicos: «SIGUE LA VOTACIÓN PARA ELEGIR LA DONACIÓN DE LULZXMAS [“Lulz navideño”]; las opciones son (en orden de ganador a perdedor): CÁNCER, TOR, SIDA, WIKILEAKS, REFUGIOS, CRUZ ROJA, ANONOPS.»

AntiSec reemplazó la página web de Stratfor’s con *The Coming Insurrection*, un opúsculo revolucionario redactado por el radical y anónimo Comité Invisible. Sus autores, obviamente franceses, que buscaban acelerar la muerte del capitalismo, convocaban a nuevas modalidades de asociación colectiva y al rápido despliegue de una «eficaz guerra de guerrillas que recupere nuestra ingobernabilidad, nuestra insumisión primordial».[263] Desde el día de Navidad hasta Año Nuevo se intensificó el ritmo de los hackeos. De conformidad con una especie generalizada de caos, AntiSec pensaba que era necesario golpear a más de una organización. Mientras la cobertura de las noticias se centraba de manera casi exclusiva en Stratfor, AntiSec había conseguido en realidad una bonanza de “hackeo de costa a costa” y así lo anunció orgullosamente en su zine:

> En vísperas de Año Nuevo, mientras los camaradas revolucionarios llevaban el ruido delante de las cárceles de todo el mundo en apoyo de los presos, nosotros abríamos fuego contra los sitios web y los correos electrónicos del 1 por ciento, publicando información robada de los departamentos de policía tanto en California como en Nueva York. De costa a costa disfrutamos del lulz mientras golpeábamos a los máximos jefes de policía: robando la información de sus correos electrónicos privados y de sus cuentas de Facebook, abusando gozosamente de sus portales internos de orden público y huyendo rápidamente con sus documentos privados que luego publicamos en servicios ocultos en tor y BitTorrent. Finalmente, desfiguramos sus sitios web y rm’d sus servidores, en vivo en el IRC y Twitter para que lo viese todo el mundo.[264]

Tres objetivos adicionales de AntiSec fueron cslea.com (la California

Statewide Law Enforcement Association, autoconsiderada, conviene señalar, como «la asociación de orden público más fascinante de los Estados Unidos»); nychiefs.org (Asociación de Jefes de Policía del estado de Nueva York); y specialforces.com (un mercado, como el nombre puede sugerir, de material orientado a las operaciones que llevan a cabo las fuerzas especiales). Cada uno de estos sitios se añadió a la creciente colección de AntiSec de colas de correos electrónicos, nombres de usuarios, contraseñas, correos electrónicos, números telefónicos y documentos «sensibles para las fuerzas de orden público».

Todo mientras Sabu continuaba con su actitud imperturbable, descarada y agresiva. En respuesta a un expartidario que acusaba de irresponsable a AntiSec, escribió con contundencia: «QUE LE DEN a la comunidad de inteligencia. la industria de seguridad. y a todos entre ambas. Nosotros apoyamos al pueblo.»[265] Describió a Stratfor como los delincuentes: «@STRATFOR ha vulnerado potencialmente la ley almacenando los datos de los clientes, sin encriptar, en una [*sic*] servidor inseguro públicamente accesible. Cuestionarlos a ellos.»[266] Las acusaciones y sospechas internas con respecto a Sabu se veían mitigadas por momentos como estos. Pero las acusaciones persistían. En Pastebin aparecieron algunos anuncios sobre esta cuestión. Uno se titulaba "Comunicado de prensa: Stratfor NO Hackea a Anonymous" y cuestionaba a Sabu: «Sabu y su equipo no son más que unas zorras oportunistas que buscan llamar la atención y posiblemente son agentes provocadores.»[267]

Apenas unas semanas antes del LulzXmas, Sabu accedió finalmente a encontrarse con Brian Knappenberger para ser incluido en el documental, pero solo si se cumplían determinadas condiciones. Sabu debía aparecer oculto y su voz tenía que ser distorsionada y Knappenberger no debía dejar ningún rastro digital de sus viajes o paradero. Debía llegar a Nueva York con el viaje en avión y el alojamiento de hotel abonados en metálico, asegurándose de que se elegía un hotel donde no necesitara identificarse. Yo estaba de vacaciones fuera de la ciudad y regresé a Nueva York (bajo un aguacero incesante) el 26 de diciembre expresamente para asistir a Knappenberger y ayudarle a ponerse en contacto con Sabu, pero nunca apareció. Sin embargo, teniendo en cuenta los importantes hackeos que se habían producido últimamente, la ausencia de Sabu parecía más un indicio de que estaba siendo prudente y no de que se había acobardado.

Al día siguiente, y a pesar de que no se había presentado a la cita, decidí hacer un último esfuerzo para ver a Sabu. Quería entregarle un pequeño regalo antes de marcharme de Nueva York, el libro *Outliers* de Malcolm Gladwell. Bajé las escaleras y llamé a Sabu, preguntándole si podía pasar al día siguiente por mi casa para recoger el regalo antes de que mi compañero y yo partiésemos hacia Canadá. Después de la lluvia y de los miserables fracasos del día anterior tenía serias dudas de que apareciera. Pero Sabu no me decepcionó. Cuando mi compañero y yo estábamos en el coche, apenas unos minutos antes de la hora prevista para emprender el viaje, apareció una enorme camioneta negra llena de tíos y Sabu saltó del vehículo. Salí del coche para ir a su encuentro. Él tenía mucha prisa y nosotros también, de modo que nuestro intercambio duró menos de diez minutos. Le di el libro y le deseé buena suerte. Sabu se acercó a nuestro coche y mi compañero bajó la ventanilla. Les presenté (evitando, según el protocolo, cualquier referencia a "Sabu" o a cualquier otro nombre; él nunca me había revelado su nombre real). Se estrecharon la mano ante la mirada atenta de nuestro viejo perro. Esa fue la última vez que vería a Sabu en persona.

Volver a los clásicos

La actividad de Anonymous se elevaría a nuevas cotas durante los tres meses siguientes. AntiSec seguía instalado en la cola de correos electrónicos de Stratfor, aportando pequeños aperitivos aquí y allá en comunicados de prensa provocadores. Entretanto, Barrett Brown continuaba mendigando los correos electrónicos, y las relaciones entre el grupo y él se volvieron tensas. Hammond me explicó que, en aquel momento, a algunos miembros de AntiSec «no les gustaba BB [Brown] por los mismos conflictos de personalidad y ego que todos ya sabemos». Algunos de ellos estaban particularmente cabreados por el hecho de que hubiese enviado tuits referidos al comunicado de prensa antes de que se hiciera público.

Ellos decidieron entregarle la cache a WikiLeaks. Hammond simplemente accedió al servidor de IRC de WikiLeaks (en gran medida a espaldas de Sabu) y el trato quedó cerrado. «Cuando hablé con WikiLeaks –me explicó Hammond– primero me pidieron que autentificase la filtración

pasteando algunas muestras, y lo hice, [pero] no me preguntaron quién era o ni siquiera cómo había tenido acceso realmente a ese material, pero les dije voluntariamente que estaba trabajando con AntiSec y que había hackeado a Stratfor.» Poco después organizó la transferencia. Cuando Sabu se enteró, insistió en que quería tratar con Assange personalmente. Al fin y al cabo, le dijo a Hammond, él ya estaba en contacto con “Q”, el asistente de confianza de Assange. (Más adelante, Kevin Poulsen, de Wired.com, publicó una historia sobre Q, un adolescente islandés, Sigurdur *Siggi* Thordarson, que en agosto de 2011 se convirtió voluntariamente en informador del FBI, con la entrega a las autoridades de miles de chats y documentos de WikiLeaks en el proceso. Thordarson lo hizo, supuestamente, «por la aventura».)[268] Sabu se metió en «conversaciones con WL sobre cómo conseguir algo de dinero por las filtraciones», según la versión de Hammond, pero para entonces WikiLeaks ya tenía los documentos en su poder y estaban en camino de ser procesados para su publicación. En apenas dos meses el público tendría acceso a esos correos electrónicos.

Cuando, aproximadamente a mediados de junio, el alboroto sobre las donaciones realizadas mediante tarjetas de crédito se apaciguó, el rostro popular de Anonymous volvió a aparecer como reacción ante la Stop Online Piracy Act (SOPA) (Acta de cese a la piratería en línea). La amplia ley de derechos de autor estadounidense era impopular y no solamente entre los libertarios civiles. Los *digerati* (personas que utilizan profusamente las tecnologías digitales para expresarse) y la élite de Silicon Valley también se alzaron contra ella. La SOPA exigía, entre otras cosas, a Google y otros buscadores que evitasen que sitios marcados, como Pirate Bay, aparecieran en los resultados de las búsquedas. Un estallido masivo y elaborado de disensión aseguró que el proyecto fuese desechado mucho antes de que pudiera ser aprobado como ley. El elemento principal fue un “día de apagón” para el 18 de enero de 2012, una protesta basada en Internet y que alcanzó una escala sin precedentes. Un puñado de grandes compañías de Internet, numerosos grupos de interés público y miles de individuos programaron sus sitios web para que solo exhibieran la pantalla en negro, con enlaces que instaban a los visitantes a escribir a sus representantes políticos manifestando su oposición a la SOPA. Alrededor de setenta y cinco mil páginas web se oscurecieron, incluidas docenas de destacados sitios web corporativos y sin fines de lucro como Wikipedia, Flickr, Wired,

4chan y Google.[269] Los periodistas también escribieron una lluvia de artículos. Menos de una semana después, la SOPA y su homóloga en el Senado, la PIPA, fueron efectivamente desechadas en forma de aplazamiento indefinido. A la postre, CBS News describió el número de participantes como «asombroso»: 4,5 millones de personas firmaron una petición que circuló a través de Google; 350.000 ciudadanos escribieron a sus representantes políticos a través de SopaStrike.com y AmericanCensorship.org; solo el 18 de junio se enviaron más de 2,4 millones de tuits relacionados con la SOPA; y una petición online enviada a la Casa Blanca reunió 103.785 nombres.[270] En respuesta a la petición, el gobierno anunció oficialmente la retirada del proyecto de ley: «Para avanzar en esta cuestión continuaremos trabajando con el Congreso sobre una base bipartidista que proporcione nuevas herramientas necesarias en la lucha global contra la piratería y la falsificación, al tiempo que defendemos enérgicamente una Internet abierta basada en los valores de la libre expresión, la privacidad, la seguridad y la innovación.»[271]

Gigantes corporativos como Google, respetadas personalidades asociadas a Internet, como el cofundador de Wikipedia Jimmy Wales, y organizaciones defensoras de las libertades civiles como la EFF fueron decisivas para alcanzar esta victoria. Pero el contingente de base de geeks y hackers también estaba presente, incluido, por supuesto, Anonymous. Ellos generaron vídeos y pósters de propaganda y aportaron actualizaciones permanentes de numerosas y prominentes cuentas de Twitter. Cuando acabó el apagón informático, los actores corporativos se retiraron rápidamente del centro del escenario. Sin embargo, Anonymous y otros continuaron la aparentemente interminable lucha.

De hecho, al día siguiente, 19 de enero de 2012, las autoridades federales organizaron el cierre de Megaupload, el popular sitio de intercambio de archivos. Kim Dotcom, el controvertido y gregario fundador de la compañía, fue arrestado durante una espectacular redada a primera hora de la mañana que se llevó a cabo en su domicilio particular en Nueva Zelanda. La eliminación de este popular sitio fue recibido de manera inquietante por los activistas de Anonymous. Aunque la SOPA no guardaba ninguna relación con el arresto de Dotcom, la acción era un recordatorio del enorme poder que podían ejercer sobre el contenido de la web las industrias vinculadas a los derechos de autor, contando o no con un respaldo jurídico

formal: aunque todavía ningún tribunal había encontrado a Dotcom culpable de piratería informática, se confiscó su propiedad y su sitio web fue desactivado de Internet. (Aunque el caso abierto contra Dotcom aún está en curso en el momento de redactar este texto, el primer ministro de Nueva Zelanda, John Key, ha presentado una disculpa pública por la vigilancia ilegal que llevó a la dramática redada en la casa de Dotcom, una acción que contó con la participación de dos helicópteros y setenta y seis agentes de policía.)[272]

Tan pronto como se conoció la noticia, Anonymous respondió con su mayor campaña de ataques DDoS realizada hasta entonces, desactivando las páginas web de Universal Music, el FBI, la Oficina de Derechos de Autor de Estados Unidos, la Asociación de la Industria Discográfica de Estados Unidos y la Asociación Cinematográfica de Estados Unidos, entre otras, entidades todas ellas que pretendían erradicar el intercambio ilegal de archivos. Anonymous y AnonOps habían decidido cambiar sus tácticas y emplearon ahora una herramienta diferente de la LOIC. Esta nueva herramienta, llamada PyLoris, tenía un diseño más inteligente y era también más potente; tal vez su rasgo más importante era que protegía la privacidad del usuario. Su mecánica consistía en establecer una conexión incompleta con el servidor de destino y luego no mantenerlo abierto durante mucho tiempo. En condiciones normales, un servidor dispone solo de unas cuantas "ranuras" para aceptar conexiones, pero si la conexión se establece solo parcialmente, la ranura esperará, rechazando mientras tanto las conexiones posteriores. Si un número suficiente de personas realizan y mantienen estas conexiones incompletas, las ranuras disponibles del servidor quedan saturadas y el servicio queda efectivamente denegado.

Todo el proceso se desarrolló como en las mejores operaciones de la vieja escuela, con el software disponible para descargarlo desde un enlace del canal de IRC y los objetivos anunciados en el canal para los varios miles de personas que optaran por el ataque. Los enlaces indicaban también instrucciones sobre la mejor manera de conseguir que las conexiones fuesen anónimas mediante el uso de Tor y VPN.

En Europa, apenas unas semanas más tarde, mientras se sucedían las manifestaciones masivas online y offline contra el Acuerdo Comercial Antifalsificación (ACTA) –otro acuerdo internacional relacionado con los derechos de autor–, Anonymous volvió a hacer acto de presencia. Después

del acuerdo del gobierno polaco para ratificar el ACTA, Anonymous se apropió de numerosos de sus sitios web y empezó a divulgar intensamente las protestas callejeras que invadían Cracovia. Poco después, los integrantes del Movimiento Palikot polaco, de tendencia izquierdista, se pusieron máscaras de Guy Fawkes durante una audiencia parlamentaria sobre el ACTA; fue la primera vez, y hasta ahora la única, que cargos electos adoptaban el símbolo revolucionario. Entre ésta y muchas otras protestas, en julio de 2012 el Parlamento Europeo rechazó la ley propuesta.

Después, uno de los Anons de la vieja guardia, que ya en otoño de 2010 había sido miembro de #command, se puso en contacto conmigo con la siguiente evaluación:

<h>: en este momento parece que hay un grupo completamente nuevo de gente
<h>: no relacionado con #antisec [y] trabajando más duro que nunca
<h>: algo que hace que me sienta feliz y orgulloso de la gente
<biella>: sí
<biella>: aquí y en algunos otros lugares
<biella>: eso es bueno
<h>: y cuando vi a esos políticos polacos
<h>: con las máscaras puestas
<biella>: sí irreal
<h>: me di cuenta de que nosotros un montón locos variopintos hemos entrado de hecho en la conciencia[ción] del mundo
<h>: y de alguna manera pequeña estamos cambiando las cosas
<h>: :D

Como participante del colectivo es natural que tratara de promocionar a Anonymous. Pero eso no era todo lo que estaba ocurriendo; su evaluación del creciente poder del grupo parecía correcta. Poco después de este intercambio recibí una llamada de un inversor de riesgo que había ayudado a organizar algunas de las protestas contra la SOPA. Quería saber más cosas sobre la forma de actuar de Anonymous entre bastidores. El grupo parecía aparecer de manera imprevisible, comentó, antes de preguntarme sobre la posibilidad que un outsider pudiera ponerse en contacto con el colectivo y utilizarlo en otras luchas por la libertad en Internet. Parecía un poco fuerte –uno de los principios básicos de Anonymous es que no será el “ejército personal de nadie”– pero, aunque solo fuera eso, su interés demostraba lo

acertado de la intuición de h: Anonymous se había convertido en un componente importante, reconocido y poderoso de la mezcla política global.

«No admitas nada, niégalo todo y contraataca»

El 27 de febrero, WikiLeaks puso a disposición de la opinión pública los correos electrónicos obtenidos de Stratfor bajo la etiqueta Archivos de Inteligencia Global. Las opiniones sobre su importancia política fueron diversas. Un pequeño grupo compuesto por periodistas, especialistas en seguridad e incluso algunos de los propios clientes de Stratfor reaccionó con un simple «bah». Afirmaron que los correos electrónicos contenían escasas pruebas de comportamiento ilegal o escandaloso. Esta reacción de indiferencia estaba teñida de la reputación poco brillante que ya tenía Stratfor en el momento de la publicación de ese material. Muchos consideraban a la empresa, en realidad, como artistas de la estafa: «Stratfor es un chiste y también lo es WikiLeaks, como para tomarlas en serio» fue el insultante titular presentado por Max Fisher en *The Atlantic*.[273] Por una suma exorbitante (hasta 40.000 dólares por año en 2001) los suscriptores de Stratfor recibían un boletín que, según Fisher, contenía poco más que un refrito de noticias. Por supuesto, la reputación de la empresa se hundió todavía más cuando se reveló que nunca se había tomado la molestia de encriptar la información de las tarjetas de crédito de sus suscriptores.

Otros periodistas y observadores en general, sin embargo, encontraron que los correos electrónicos eran políticamente potentes y aportaban indicios sólidos de que Stratfor se beneficiaba de prácticas moralmente dudosas, tales como la propaganda corporativa disfrazada de comunicación y la vigilancia de activistas. Los correos electrónicos de Stratfor son realmente reveladores y a veces premonitorios. Tomemos, por ejemplo, el siguiente extracto de un correo electrónico más extenso que fue enviado, sorprendentemente, a través de un iPhone el 10 de diciembre de 2010:

> Los chaners/anon/b son instruidos y están a la vanguardia de la tecnología basada en la red, disponen de una estructura nebulosa de personas leales repartidas por todo el mundo sin ningún fundamento

> nacionalista trocito [*sic*] unidas bajo un interés común en el caos (*hentai* [anime de contenido porno] y gatos, no te jode). Hay numerosos ejemplos en los que han revelado identidades y un montón de datos personales de gente basándose en una única foto (de una mujer metiendo a un gato en un cubo de basura por ejemplo) y comprado [*sic*] un estilo serio de justicia vigilante a aquellos con los que no están de acuerdo...
>
> Será muy interesante ver qué hace un Anon en el entorno 'post-wilileaks' [*sic*]. Si pasaran de ser un grupo de geeks tecnológicos en el sótano de mamá a convertirse en un movimiento real podrían provocar problemas serios y resultar difíciles de matar. La coresía [*sic*] no es el problema pero el puñado de trastornados que hay entre ellos podrían resultar muy destructivos si se lo proponen.[274]

El periodista Steve Horn examinó miles de correos electrónicos de Stratfor y escribió una serie dividida en dos partes en las que analiza las tácticas aplicadas por la empresa y sus predecesores, Mongoven, Biscoe y Duchin (MBD) y Pagan. El fundador de MBD, Ronald Duchin –un militar con una vasta experiencia en el ámbito de la comunicación– planteó la llamada "fórmula Duchin": «aislar a los radicales, 'cultivar' a los idealistas y 'educarles' para que se conviertan en realistas. Luego cooptar a los realistas para que estén de acuerdo con la industria.» Horn observa que esta estrategia «la sigue empleando Stratfor hasta la fecha».[275]

La mayoría de correos electrónicos de la empresa muestra que «el servicio más importante que presta Stratfor es su análisis sociológico al servicio del capital y el poder corporativos, no el trabajo sucio sobre el terreno», según Horn.[276] Unos cuantos correos electrónicos señalan también una implicación más directa en la vigilancia de los activistas. Una explosión ocurrida en 1984 en la planta de Union Carbide India Limited en Bhopal, India –uno de los peores desastres industriales del siglo XX– dejó un saldo de miles de muertos y más de 500.000 personas expuestas a los efectos de sustancias químicas mortales. Dow Chemical, que posteriormente compró Union Carbide, contrató a Stratfor para que les mantuviese informados sobre los distintos grupos de activistas, tales como los Yes Men y Bhopal Medical Appeal, que se dedicaban a divulgar el problema o a asistir a las

víctimas. Los documentos revelaban que Coca-Cola había contratado los servicios de Stratfor para que vigilase al grupo ecologista PETA, especialmente sus operaciones en Canadá durante el período previo a la celebración de los Juegos Olímpicos de invierno de Vancouver. Y Stratfor envió a uno de sus empleados, al que se describe en uno de los correos electrónicos como “U/C” (encubierto), para que se infiltrase en el grupo local de Occupy en Austin, Texas, con el propósito de reunir datos de la organización, seguir los movimientos de los integrantes y detectar posibles vínculos con activistas ecologistas:

> Hay un grupo con el que es posible que estéis familiarizados llamado Deep Green Resistance [...] Si alguien en los federales o en otra parte clasifica a este grupo como ecoterrorista o no, no lo sé, pero no son más que eso y deberían ser vigilados... La sección local de Austin formó parte de la multitud de Occupy en el ayuntamiento de Austin, sin embargo, las cosas no fueron lo bastante “radicales” para ellos ya que no creen en el trabajo dentro del sistema. Cuando yo estaba trabajando como U/C, el 5 de noviembre, algunos de mis contactos me hablaron en la Asamblea General del 4 de noviembre de conflictos entre la gente habitual de Occupy y Deep Green.[277]

Estos ejemplos evocan las cuestiones tratadas en el Capítulo 7 con respecto a los correos electrónicos de HBGary y HBGary Federal que, entre otras sugerencias a la vez espeluznantes e invasivas, contenían una propuesta para desacreditar a WikiLeaks. La información relativa al espionaje corporativo, incluso con la aportación de estos correos electrónicos, sigue siendo escasa. No obstante, entre los crecientes ejemplos de abusos y la dificultad de acceder a los registros corporativos, deberíamos, como mínimo, preocuparnos por la revelación de los cálidos vínculos que existen entre la industria privada y el gobierno. Si efectivamente –como sugiere uno de los correos electrónicos– el vicepresidente de inteligencia de Stratfor, Fred Burton, se rige por el código «No admitas nada, niégalo todo y contraataca», entonces podemos ver la importancia que tienen las filtraciones y las actividades de denuncia de Anonymous y los de su clase.

Stratfor publicó esta declaración en relación a la autenticidad de los correos electrónicos filtrados:

> Algunos de los correos electrónicos pueden haber sido falsificados o alterados para incluir imprecisiones; algunos pueden ser auténticos. No validaremos ninguno de ellos. Tampoco explicaremos el razonamiento que incluyen. Habiendo sido víctimas de un robo, no queremos ser victimizados dos veces sometiéndonos a un interrogatorio sobre ellos.[278]

Stratfor, sin embargo, sí hizo comentarios sobre dos correos electrónicos que más tarde fueron ampliamente aceptados como fraudes: una carta de dimisión del fundador, Director de Informática y Director Ejecutivo de Stratfor, George Friedman, que redactó AntiSec, y un correo electrónico fraudulento supuestamente enviado a todos los clientes de Stratfor ofreciéndoles una suscripción gratis al boletín publicado por la empresa a modo de oferta de paz y disculpa por la violación sufrida por su sitio web.

«Necesitaba la verdad ahí fuera»

Aproximadamente en esa época, Sabu se volvió más fanfarrón y desafiante que nunca en público. A comienzos de febrero, en respuesta a un crítico que preguntaba por el estado de los correos electrónicos sirios que, según los rumores, tenía AntiSec en su poder, Sabu ladró: «Tendrás que comerte tus palabras una vez que decidamos filtrar lo que tenemos. Nos importan una mierda los gobiernos. Solo nos importa el pueblo.»[279] No había hablado con él desde que me mudé a Canadá. Esto no se debía solamente a la logística del traslado; llamar desde un teléfono público al aire libre en pleno invierno en Montreal te expone a quedarte congelado. Pero el 6 de marzo, a primera hora de la mañana, Sabu siguió acosándome a través de Twitter. No le importaba qué medio eligiera para ponerme en contacto con él, solo que lo hiciera y lo antes posible. Cogí el teléfono de casa y le llamé.

Fue como si comenzara a hablar incluso antes de levantar el auricular: «Fox va a publicar un artículo sobre mí y el FBI.» Sabu me explicó que estaba previsto que el artículo saliera a la luz en pocos minutos. Dijo que quería explicarme algunas cosas antes de que yo leyera el texto. Angustiado, dijo que Fox se había «rebajado mucho» para llegar hasta él y su familia, pero se negó a decirme qué era lo que habían hecho

exactamente. Solo dijo, «No es lo que estás pensando». La cabeza me daba vueltas con todo ese asunto; empecé a marearme. Recuerdo que estaba furiosa y tenía dificultades para verbalizar lo que sentía en ese momento o para recordar lo que Sabu decía. Y entonces, de alguna manera, la conversación terminó.

Resultó que no había uno sino tres artículos sobre Héctor Xavier Monsegur, cada uno de ellos acompañado de una fotografía gigante de su rostro mientras estaba sentado delante de un ordenador. Allí estaba: la cooperación de Sabu con el FBI. Esto era lo que había estado tratando de decirme por teléfono. Yo estaba estupefacta. La noticia coincidió con una serie de acusaciones detalladas también en el artículo. En Estados Unidos, el FBI acababa de arrestar a Jeremy Hammond, mientras que en el Reino Unido e Irlanda se presentaron cargos de conspiración informática contra Ryan Ackroyd (Kayla), Donncha O'Cearbhaill (Palladium) y Darren Martyn (pwnsauce).

La noticia se propagó como una onda expansiva a través de los diferentes canales de IRC. El canal CabinCr3w alojaba a muchas personas muy próximas a Sabu (se han cambiado los seudónimos):

<round-eyes>: camarada, primera página de Foxnews
<round-eyes>: ahora
<kama>: ok
<round-eyes>: omgomgomg
<flava-flav>: joder
<flava-flav>: no lo sabía
<flava-flav>: guau
<flava-flav>: puto sabu
<flava-flav>: tíos
<flava-flav>: puedo hablar
<flava-flav>: un minuto
<Nacho-King>: adelante
<Mega>: NO
<Mega>: lol estaba bromeando adelante
<comrade>: lol
<flava-flav>: deberíamos enmarcar esto como un momento decisivo
<Nacho-King>: ^
<flava-flav>: como libia después de gadaffi
<flava-flav>: nos hemos librado de una carga

<flava-flav>: un peso muerto
<flava-flav>: empañando todo lo que éramos
<flava-flav>: y seremos
<Mega>: bueno él nunca fue una carga para empezar en mi opinión
<comrade>: si, eso es extrañamente incómodo en este momento flava-flav
<flava-flav>: y desde ahora
<Mega>: por qué no camarada
<flava-flav>: no entiendes lo que quiero decir
<flava-flav>: él era una fase
<flava-flav>: y ahora
<comrade>: lol
<flava-flav>: es otra nueva
<comrade>: de acuerdo
<comrade>: puedo aceptar la fase
<comrade>: :D
<flava-flav>: es [un] proceso evolutivo
<Nacho-King>: exacto solo digo flava-flav que un montón de gente está reaccionando de muchas maneras diferentes

Nacho-King tenía razón. Mientras que todo el mundo sentía el amargo aguijón de la traición, una minoría seguía apoyando a Sabu. De hecho, el artículo aparecido en Fox News informaba que el FBI había agitado ante Sabu un ultimátum honorable: podía trabajar con los hombres del gobierno o, de lo contrario, le quitarían a la fuerza la custodia de sus dos primas adoptadas. Finalmente, un grupo de exparticipantes de Anonymous –más simpatizantes que hackers de la línea dura– me dijeron que Sabu, ya en el verano de 2011, les había estado insistiendo en que «se largasen de allí». Comenzó a estar cada vez más claro por qué Sabu había estado coqueteando con los Anons que poseían las habilidades de hackeo necesarias para acceder a los sistemas, y no le preocupaban en absoluto aquellos que no estaban violando la ley. Estaba apuntando a aquellos que más le interesaban al FBI.

Unas horas más tarde empezó a surgir en los canales una actitud dominante, una actitud que reflejaba el sentimiento de un funcionario del gobierno anónimo citado en el informe de la Fox: «Tal vez sea un mesías en la comunidad hacker, pero sigue siendo un chivato.»

En última instancia, la reputación de Sabu dentro de Anonymous estaba irrevocablemente manchada. Y cuando la noticia reverberó a través

de las tripas de Internet se escucharon aullidos de cólera y punzadas de traición. Pasó un mes hasta que mi ira se disipó lo suficiente como para poder volver a mantener una conversación con él. Sabu estaba en su actitud más desafiante y comenzó nuestra conversación con la salva de que estaba «decepcionado de que nadie hubiera cuestionado el boletín de noticias». Luego lanzó un gruñido de incredulidad al ser tratado como un “peligro biológico”.

«He protegido a cientos de personas –insistió–. Le he salvado el culo a un montón de gente. Cuando tienes hijos, tienes que elegir. Hice lo correcto.» Su única petición de comprensión se refería al hecho de que él también debía hacer frente a un castigo. Al fin y al cabo, había sido arrestado y conservaba su libertad solo bajo fianza, pero seguía vigente la posibilidad de que tuviese que enfrentarse a diez o quince años de prisión. No saber cuál será tu destino es «estresante», dijo. Cuando le pregunté cuánto de lo que había hecho y dicho estaba dirigido por el FBI, respondió con vehemencia: «Todo lo que dije en Twitter era mi puto punto de vista.» Luego añadió: «En mis tuits era auténtico, nadie dictaba lo que escribía.» Eso contradice directamente las declaraciones hechas por su controlador, según informó Jana Winter para Fox News. «Alrededor del 90 por ciento de lo que vemos online es mentira»,[280] dijo el controlador, en referencia tanto a los posts como a la cuenta de Twitter de Sabu, y también a las “entrevistas” que concedió a la prensa. Sea esto verdad o forme parte de una campaña de desinformación incluso más elaborada y recursiva, la implicación subyacente es que Sabu repitió como un loro todo lo que el FBI quería que dijese. Había algunos tuits –«Si dios impide que sea arrestado, admitiré todos mis delitos y me entregaré yo mismo. No creo en hacer pagar a otras personas por mis propios pecados. Gracias»– que ahora sabemos que eran cápsulas sin adulterar de mentiras influidas por el FBI.[281]

Apenas si tuve oportunidad de abrir la boca, pero aun así conseguí preguntarle a Sabu si se había reunido conmigo a instancias del FBI. Su tono de voz se elevó rechazando rotundamente mi sugerencia. «¡Por Dios bendito! ¡No necesitas pedir permiso para ir al puto *Chipotle* y pedir un burrito!» No satisfecha con su respuesta volví a preguntarle por qué se había puesto en contacto conmigo, y le hice una pregunta más sobre el catalizador de nuestro encuentro, el hacker que me abordó en la reunión del NYSEC. Comenzó quitándose de encima ese asunto antes de interrumpirse

súbitamente. «Necesitaba saber la verdad de una manera u otra –afirmó con rotundidad–. Cuanto más tiempo pasábamos juntos, más sentía que podía confiar en ti. Es una situación de mierda.»

Sabu lanzó una última lluvia de vitriolo: «Esperaba que fuesen los nerds quienes expusieran a mi familia, no los medios de comunicación. ¡Porque fueron los medios los que echaron mierda sobre mi familia!» Y añadió: «En Anonymus hay muchos chivatos.» Luego acabó su intervención con algunos agradecimientos y mostrando su reconocimiento «a Jeremy y Donncha», dos de los hackers más trabajadores y técnicamente dotados de Anonymous, quienes se habían negado a proporcionar ninguna información a las autoridades policiales (y cuya captura había sido consecuencia en buena parte de las acciones de Sabu). Luego pronunció algunas palabras de despedida: «Sigo pensando que la idea de Anonymous es hermosa. La descentralización es poder.»

La violación de la ley y los chivatos

Alrededor de esta época, los participantes de Anonymous y algunos periodistas independientes como Nigel Parry empezaron a plantear interrogantes acerca de la historia oficial que se había montado en torno al hackeo perpetrado contra Stratfor. El 25 de marzo de 2012, Parry escribió un detallado blog titulado “Sacrificar a Stratfor: Cómo esperó el FBI tres semanas para cerrar la puerta del establo”.[282] Parry observó lo extraño que era que la minuciosa operación contra Stratfor pudiese llevarse a cabo bajo las mismas narices del FBI. Después de todo, el FBI sostenía –tanto en los documentos legales como en el informe presentado por la Fox– que Monsegur estaba perfectamente controlado todo el tiempo. «El FBI –escribió Jana Winter– ha tenido a un agente vigilando su actividad en la red veinticuatro horas al día, según los agentes del gobierno.»[283]

Monsegur proporcionaba al FBI un acceso directo y en tiempo real al desarrollo de los acontecimientos y el FBI informó casi de inmediato a Stratfor de la intrusión, a principios de diciembre. AntiSec solo tuvo acceso a la base de datos de los clientes de la empresa en ese momento. A Hammond le llevó otros diez días infiltrarse en el resto del sistema; Hammond no borró los datos hasta diez días más tarde, en Nochebuena.

Stratfor dispuso de una oportunidad más que suficiente para mejorar su seguridad o, al menos, de hacer copias de seguridad de sus datos. Pero no hizo nada de esto. Una vez producido el ataque, George Friedman, Director Ejecutivo de Stratfor, ofreció la siguiente y vaga explicación: «Trabajamos para mejorar nuestra infraestructura de seguridad dentro de las limitaciones impuestas por el tiempo y por el deseo de proteger la investigación, no permitiendo que los atacantes supieran que conocíamos su intrusión.»[284]

Hacia noviembre de 2013 las actas judiciales de acceso público habían confirmado la cronología expuesta por Hammond. Y, sin embargo, durante más de dos años ningún otro periodista se molestó en presionar a Stratfor por su fallo al no haber tomado medidas preventivas adicionales después de la intrusión inicial. Tampoco se preguntaron por qué había esperado el FBI hasta el 24 de diciembre para proporcionar a Stratfor una segunda oleada de malas noticias –que se habían descargado los correos electrónicos y se estaban borrando los datos– cuando se sabía perfectamente que días antes AntiSec había conseguido un amplio acceso al sistema.

La racionalización del FBI para explicar sus acciones no aclara en absoluto la situación. Tal como informó Nicole Perlroth de *The New York Times*: «El FBI manifestó que notificó inmediatamente a Stratfor, pero añadió que entonces ya era demasiado tarde. A lo largo de las semanas siguientes, los hackers escarbaron en la información financiera, los correos electrónicos y la información financiera y personal de los suscriptores de Stratfor, borrando ocasionalmente sus datos más valiosos, y todo esto a la vista de los agentes del FBI.»[285]

Entonces, en mayo de 2014, un montón asombroso de documentos legales –registros de chats, fotografías de vigilancia y documentos del gobierno pertenecientes a la causa judicial de Hammond– fue filtrado a los periodistas Dell Cameron y Daniel Stuckey. Provistos de este material, Cameron y Stuckey pudieron corroborar la cronología de Hammond con mucho más detalle. Los registros de chats, en particular, confirman en gran medida, como escribió Cameron, «las antiguas acusaciones de que los investigadores federales permitieron que un informador violase repetidamente las leyes contra los delitos informáticos mientras buscaban a Hammond y a otras figuras relevantes de Anonymous»[286]

Las acusaciones de que Sabu contribuyó a cometer actividades ilegales y las instigó (recordemos que Sabu fue quien reveló inicialmente a

Hammond la vulnerabilidad de Stratfor) no se limitaron al hackeo de Stratfor. Durante la celebración de la audiencia de sentencia de Hammond, en noviembre de 2014, éste leyó una declaración que incluía otra acusación explosiva:

> Después de Stratfor, continué penetrado en otros objetivos utilizando un poderoso "exploit del día cero" que me permitió un acceso de administrador a sistemas que ejecutan la popular plataforma que aloja el servicio de instalación de Plesk. Sabu me pidió varias veces tener acceso a este exploit, pero no se lo permití. Sin su propio acceso independiente, Sabu siguió proporcionándome listas de objetivos vulnerables. Penetré en varios sitios web cuyos datos él me suministró, subí las cuentas de los correos electrónicos y las bases de datos robados al servidor del FBI de Sabu y entregué contraseñas y puertas traseras que le permitieron a Sabu (y, por extensión, a sus controladores del FBI) hacerse con el control de estos objetivos. Estas intrusiones, todas las cuales fueron sugeridas por Sabu mientras cooperaba con el FBI, afectaron a miles de nombres de dominios y que consistían en su gran mayoría en sitios web de gobiernos extranjeros, incluidos los de Brasil, Turquía y Siria.[287]

Cuando Hammond estaba a punto de mencionar más objetivos gubernamentales, el juez Preska le suplicó: «Señor Hammond, acabamos de hablar de que la mención de esos países ha sido censurada, le agradecería que no los utilizara.» En su declaración, Hammond también recordó al tribunal la existencia de algunas pruebas que avalaban sus alegaciones:

> Todo esto sucedió bajo el control y la supervisión del FBI y puede ser confirmado fácilmente por los registros de chates que el gobierno nos proporcionó de acuerdo con las obligaciones derivadas de los hallazgos del gobierno en el caso contra mí... Como me declaré culpable no tengo acceso a muchos documentos que se me podrían haber facilitado antes del juicio, tales como las comunicaciones mantenidas por Sabu con el FBI. Además, la mayoría de los documentos que me entregaron se encuentra bajo una "orden de protección" que priva a este material del escrutinio público.

La declaración de Hammond fue reeditada online y algunos sitios web censuraron los nombres de los países mencionados, mientras que otros los incluyeron. Como me había enterado previamente de estos hackeos durante mi primera visita a la prisión, me intrigaba cuánto de verdad podía haber detrás de las alegaciones de Hammond. Les planteé estas cuestiones a algunos periodistas y convencí a uno de ellos para que les siguiera la pista. Finalmente este asunto acabó en un artículo de primera página en *The New York Times* a finales de abril de 2014, firmado por Mark Mazzetti y titulado "Informador del FBI vinculado a ciberataques en el extranjero".[288] Más tarde, cuando ya se había filtrado el botín de documentos legales bajo orden de protección, los periodistas Daniel Stuckey y Andrew Blake escribieron un detallado artículo sobre el papel desempeñado por Sabu en la planificación de hackeos contra el gobierno de Brasil y numerosos sitios web corporativos. Aunque muchos de los objetivos de Sabu eran hilvanados a través de Hammond, también les facilitó vulnerabilidades a otros hackers. En un caso documentado ofreció un valioso exploit que «abrió puertas traseras para colarse en cientos de sitios web brasileños».[289] Y todas estas operaciones se llevaron a cabo bajo la atenta mirada del FBI.

La noticia de que el FBI había permitido –o al menos tolerado– el papel de Sabu en la facilitación de un festival de hackeos ilegales cayó entre muchos integrantes de Anonymous como un perverso abuso de poder. Por supuesto, no sabemos –y es probable que nunca lo sepamos– si los servicios prestados por Sabu fueron cedidos por el FBI a otras agencias de tres letras para llevar acabo operaciones militares, o para recabar información de inteligencia, si sus acciones favorecieron los propósitos del gobierno de alguna manera indirecta, o si había otros factores encima de la mesa; pero cuando este ejemplo se contextualiza dentro del amplio sistema de informadores estadounidense resulta evidente que el caso dista mucho de ser inusual. La profesora de Derecho Alexandra Natapoff sostiene que las relaciones corruptas entre los informadores y sus controladores no son actividades esporádicas o excepcionales, sino que son endémicas. En su libro *Snitching*: *Criminal Informants and the Erosion of American Justice,* describe de manera convincente un sistema retorcido que a menudo produce ciclos crecientes de crimen y violencia. El FBI permite rutinariamente que sus informadores vulneren la ley, afirma Natapoff, siempre que se muestren dispuestos a cooperar. Si bien los informadores son una herramienta

necesaria para el sistema de justicia penal, la autora llega a la conclusión de que, según la configuración actual de los programas, «el uso de informadores inflige importantes heridas a la integridad del proceso penal».[290]

Natapoff y otros periodistas han documentado numerosos casos de abusos. Por ejemplo, en 2005, Yassine Ouassif, un estudiante de ingeniería a tiempo parcial que vivía en la Bahía de San Francisco, fue obligado a bajar de un avión en París con destino San Francisco. A pesar de disponer de carta verde y no estar bajo investigación, Ouassif fue interrogado durante horas en unas instalaciones del Servicio de Aduanas y Protección de Fronteras estadounidense. Al final, un agente del FBI le ofreció una alternativa: convertirse en informador en la comunidad musulmana estadounidense o ser deportado a su país natal, Marruecos.[291] Una demanda presentada en abril de 2014 en nombre de cuatro hombres musulmanes alega que el FBI les colocó o mantuvo en una lista de exclusión aérea después de que se negasen a espiar a las comunidades musulmanas de Nueva York, Nueva Jersey y Nebraska.[292] Esta clase de intimidación pretende intervenir directamente en una comunidad, alterando su propia naturaleza sin haber establecido formalmente la comisión de ninguna ilegalidad.

En Estados Unidos, la mayoría de los casos que involucran a informadores nunca llegan a juicio, de modo que en gran medida aprendemos acerca de este sistema –y somos capaces de argumentar para que se corrija– gracias a los juicios y filtraciones ocasionales (y eso nos recuerda cómo la filtración de la causa judicial de Hammond puede servir al proceso democrático). El hecho de que a Sabu se le permitiera facilitar tantos hackeos a la vista del FBI es una prueba que demuestra los abusos continuos del sistema de informadores. También sirve como doloroso recordatorio de que el estado empleará métodos legales e ilegales para desmantelar a un movimiento al que considera una amenaza.

«Nunca confíes en nadie en el IRC»

A medida que se propagaba la noticia sobre el estatus de informador de Sabu, se volvió evidente que, si bien la cooperación prestada por Monsegur

había marcado una diferencia decisiva, muchos participantes no habían tomado las medidas adecuadas para proteger su información. Anonymous9 lo expresó de esta manera: «El hecho de que arresten a la gente por su causa se debe, en parte, a que era un traidor y, en parte, a que esa gente era descuidada. Si ellos no hubieran compartido información personal con él, no habrían tenido problemas. Es algo así como volver a la cuestión de 'nunca confíes en nadie en el IRC'.»

Demostrar delitos informáticos puede resultar difícil después de que se hayan cometido, a menos que se encuentren datos en el ordenador del sospechoso, tales como números de tarjetas de crédito, correos electrónicos u otra información incriminatoria. Pero según el investigador en seguridad Robert Graham, los registros de chats extraídos por un informador se pueden utilizar para «condenarte por conspiración, intención u obstrucción de la justicia [y] chantaje».[293] Y el fiscal tenía en su poder una enorme cantidad de registros con los cuales construir su caso. No obstante, tener a Sabu no bastaba para detener a todo el mundo, y algunos miembros de AntiSec y LulzSec continúan fuera del alcance de la ley. Si otros hackers hubiesen sido más cuidadosos con su seguridad operativa es posible que nunca les hubiesen atrapado.

¿Cómo se cometieron los errores? Hammond puso en práctica una seguridad operativa técnica casi perfecta, pero en sus chats reveló detalles personales. El más importante de ellos –que yo le oí mencionar una vez en público y otra vez en un canal privado– fue que había pasado algún tiempo en una prisión federal. Teniendo en cuenta uno de sus principales apodos, *Anarchaos*, su estatus único como uno de los pocos hackers anarquistas estadounidenses que había pasado tiempo en prisión en los Estados Unidos, seguramente le colocó en un lugar privilegiado en la lista de candidatos. Tal vez la única tarea vital que Sabu llevó a cabo para el FBI en este caso fue la de conectar el pupurrí de apodos diferentes que utilizaba Hammond. A continuación se muestra un fragmento de una conversación, archivado en los documentos legales, entre Sabu (como "CW-1") y Hammond (como "@sup_g") el día de Navidad:

<CW-1>: ¿cómo pintan las noticias?
<@sup_g>: He estado trabajando duro toda la noche
<CW-1>: He oído que estamos en todos los periódicos

<CW-1>: vosotros cabrones conseguiréis que me allanen la casa
<CW-1>: JAJAJAJA
<@sup_g>: publicamos 30k de tarjetas, el contenido de it.stratfor.com y otra declaración
<@supg>: tío, es la bomba
<CW-1>: si me cogen anarchaos vuestro trabajo es causar estragos en mi honor
<CW-1>: te quiero
<CW-1>: sup_g:
<@sup_g>: así se hará

Sabu, por supuesto, demostró de muchas otras maneras ser una pieza fundamental para las investigaciones: un miembro de LulzSec compartió un enlace a un vídeo casero que colgó en YouTube. Con la URL, las autoridades enviaron una citación a YouTube para que entregase la dirección de correo electrónico de la cuenta, y a partir de allí fue muy sencillo conectarse a su cuenta de Facebook. Este joven hacker había cometido el grave error de subir capturas de pantalla incriminatorias de la desfiguración de un sitio web que luego compartió con otro miembro de LulzSec (oy vey).

La sugerencia de Anonymous9's de «no confiar en nadie en el IRC» es mucho más fácil de expresar que de poner en práctica. El "sabutaje", como lo describió alguien en tono humorístico, afectó de un modo tan profundo porque Anonymous, como casi todos los movimientos políticos, estaba suscrito por amistades e incluso la eclosión de relaciones más íntimas. Los matrimonios, como el del joven hacker John Anthony Borell III (Kahuna), de CabinCr3w, y su esposa Sarah, tuvieron su origen en chats compartidos en el canal privado de IRC del grupo. Topiary acompañó a uno de sus colegas LulzSec a través de un oscuro período de su vida. Incluso aquellos que nunca habían compartido información de identificación personal se vieron implicados en vínculos sólidos y duraderos. Dichas conexiones hacían que resultara demasiado tentador, y fácil, caer en un estado de bienestar en el que uno traiciona su identidad debido a que comparte en exceso. Incluso si se reconoce que esto realmente está ocurriendo, no es tan sencillo como cambiarse el apodo, borrar todos los indicios de la identidad anterior y adoptar un estilo de conversación diferente. Parmy Olson destaca este "dilema" al que deben enfrentarse continuamente los hackers: cambiar un apodo significa perder las señas de identidad y una reputación estables

que son fundamentales para el trabajo cooperativo del hacker a lo largo del tiempo.294

Unos años más tarde les pregunté a algunos Anons por qué –teniendo en cuenta las crecientes sospechas de que era un informador de las autoridades– Sabu no solamente era tolerado sino que, de hecho, era presentado como el rostro público de AntiSec. Para O'Cearbhaill, uno de los otros Anons de AntiSec, su carisma daba sus frutos. Era capaz, como ningún otro, de despertar la pasión pública con sus toques de corneta a la sublevación. Otros numerosos participantes ofrecieron explicaciones verosímiles: otra figura, Yettie (no es su seudónimo verdadero) fue durante mucho tiempo el objetivo de abundantes acusaciones de ser un chivato, una circunstancia que desvió el punto de mira de Sabu. Al menos una docena de sus participantes principales había compartido conmigo sus temores respecto de Yettie. Él había conseguido acceder a innumerables servidores de IRC y era conocido por jugar con las mentes de muchas personas, creo que incluida la mía. Hasta Hammond, que operaba momentáneamente bajo el handle de "crediblethreat", se puso en contacto con Yettie en el otoño de 2011 en una inusual exposición pública de una disputa interna:

<crediblethreat>: hola Yettie
<crediblethreat>: le contaste a todo el mundo
<crediblethreat>: sobre cómo y por qué te expulsaron del equipo principal de antisec?
<crediblethreat>: ¿dónde estabas tú todos estos meses?
[...]
<crediblethreat>: ¿por qué coño debería nadie volver a confiar en ti, chivato?

Hasta el día de hoy nadie puede decir con absoluta seguridad si Yettie es un informador (o simplemente espantoso). Muchos otros también fueron acusados de soplones. Esta clase de rumores es analizada interminablemente a la luz de lo que se considera como un comportamiento extraño y de la escasa información objetiva disponible para los participantes. Por ejemplo, en los documentos de las autoridades oficiales filtrados se nombra a "CW-2" (testigo colaborador 2), lo que implica que había al menos dos informadores colaborando con ellos (y, teniendo en cuenta otros documentos, el número de informadores es de al menos cinco).295 Muchos participantes también preguntaban por qué algunos

participantes incorporados a los canales secretos nunca eran sometidos a allanamientros o interrogatorios tras decidir aparecer públicamente. Estos rumores e incertidumbres alimentan la atmósfera de paranoia tormentosa y desconcertante tan habitual en el contexto de los movimientos políticos de izquierda o progresistas; una vez se asienta la niebla del temor y la inseguridad, «resulta difícil distinguir la paranoia de la realidad, a los enemigos imaginarios de aquellos que son perfectamente reales», en palabras de Ruth Rosen, quien describió el temor inducido por el FBI en la década de 1960 en el movimiento de liberación de la mujer.[296]

La revelación de las actividades de Sabu funcionó también como una prueba, empujando a Anonymous hacia un período de introspección. A lo largo de las semanas, mientras en Anons se lamentaban, bramaban, evaluaban, reconsideraban y se volvían locos en Twitter y en diferentes redes del IRC, se preguntaban al mismo tiempo qué futuro –en el caso de que tuviese alguno– le esperaba a Anonymous después de un golpe semejante. ¿Acaso ocurriría, para citar a un funcionario anónimo del gobierno presentado en el artículo de Winter en Fox News, que «cuando la comunidad de los hackers se de cuenta de que su Dios en realidad ha sido la cooperación [*sic*] con el gobierno, se producirá el terror puro»?

TOC, TOC, ESTAMOS AQUÍ

Si bien el sabutaje avivó las llamas de la paranoia, eso no significó el final de Anonymus ni provocó siquiera una cantidad sustancial de terror. Aunque nunca pudo reproducir los elevados niveles de participación de sus días de LulzSec/AntiSec (aquella época en la que la descripción que hizo de ellos Fox News como “hackers chutados de esteroides” era acertada), Anonymous funcionó bastante bien durante 2012 y buena parte de 2013, ejecutando hackeos y ataques en todo el mundo. Su formidable reputación queda perfectamente ilustrada por una anécdota de las más altas esferas oficiales de Estados Unidos.

En 2012, el equipo de la campaña para la reelección de Barack Obama reunió a un grupo de programadores, administradores de sistemas, matemáticos y científicos de datos para afinar la orientación de los votantes. Los periodistas elogiaron el equipo tecnológico de Obama, heterodoxo y

plagado de estrellas, detallando el duro trabajo, el éxito y las tribulaciones de sus miembros y, finalmente, anunciando el sistema como un acierto. Estos artículos, sin embargo, no informaron de uno de los mayores problemas que tenía el equipo. A lo largo de la campaña, los tecnólogos habían tratado a Anonymous como una molestia potencialmente incluso mayor que los hackers de países extranjeros que se habían infiltrado en las campañas de McCain y Obama en 2008.[297]

A finales de noviembre de 2012, Asher Wolf, un periodista y cruzado geek, observó que Harper Reed, el director tecnológico del equipo técnico para la reelección de Obama, seguía a @AnonyOps en Twitter. De una manera muy parecida a la empleada por un embaucador, Wolf advirtió de esta circunstancia a AnonyOps, sugiriendo, «juguemos con esto y veamos qué podemos hacer».[298]

AnonyOps envió a Reed un mensaje privado a través de Twitter. «Hola. Los próximos meses son importantes. Pensé que quizás deberíamos hablar.» Reed leyó el mensaje y «el corazón le dio un vuelco», según me explicó en una entrevista. Fue a ver a su jefe, el director de información, y al jefe de seguridad de la campaña de Obama. Los tres barajaron varias respuestas posibles en 140 caracteres. Finalmente coincidieron en esta concisa obra maestra: «Hola. ¿En qué has pensado?» Cuando Harper estaba a punto de enviar el mensaje, el director de información, que había estado hablando con prestigiosos abogados de la campaña, corrió hacia el escritorio de Harper para detenerle. Habían cambiado de idea. La mejor respuesta, decidieron, era no dar ninguna respuesta. Pero llegó unos segundos demasiado tarde.

Si Reed hubiese sabido lo que yo sabía, se habría ahorrado uno o dos días de ansiedad. AnonyOps simplemente estaba interesado en iniciar una conversación con una figura política influyente. Reflexionando sobre este asunto durante una entrevista conmigo, Wolf recordó que

> era divertido, porque éramos como críos jugando al límite [...] con la superpotencia mundial. Habíamos pasado 2010, cuando las pantallas rebosaban de furia cuando la administración fue a por WikiLeaks, y habíamos pasado Occupy [...] Habíamos visto a gente encarcelada, desaparecida... Tal vez, solo tal vez, éramos un tanto fatalistas. Y tal vez disfrutábamos por una vez, por una sola vez, del hecho de vagar

> cerca de la administración que mata niños pequeños con drones y arrojarles una colilla a la cara.

Como muestra este incidente, Anonymous se había convertido en un espectro; su influencia se había vuelto tan trascendental que ni siquiera necesitaba hacer nada para provocar un efecto. Es comprensible que el equipo que trabajaba para la reelección de Obama se sintiera perturbado por esta llamada ambigua a su puerta digital. En los dos meses posteriores al arresto de Hammond, Anonymous hackeó cientos de sitios web del gobierno chino; desactivó el sitio web de las carreras de Fórmula 1 después de que el gobierno represivo de Bahrein, país designado como sede de la siguiente carrera de Fórmula 1, hubiese detenido y encarcelado a manifestantes; y hackeó el sitio web del ministro de finanzas griego, llamando la atención sobre el plan del gobierno heleno de rastrear la información bancaria de los ciudadanos en un esfuerzo por reducir el fraude fiscal. Durante el verano de 2012, Anonymous lanzó otro ataque importante (nuevamente) contra el sitio web de la Fórmula 1, en esta ocasión coincidiendo con el Gran Premio de Montreal; la acción se llevó a cabo para protestar contra Bill 78, una medida controvertida aprobada en Quebec y destinada a restringir las actividades de protesta, que se habían disparado después de que se propusiera un aumento de las tasas de las matrículas. La Comisión de Derechos Humanos de Quebec publicó un informe de cincuenta y seis páginas condenando el proyecto de ley por su flagrante violación de la propia carta de derechos humanos de la provincia, principalmente por la disposición que amenazaba con multar a los manifestantes con miles de dólares si no comunicaban a las autoridades, al menos con ocho horas de antelación, el itinerario de cualquier manifestación de protesta que incluyera a cincuenta o más personas.[299] En la India, aquel mismo mes, después de que una orden del Tribunal Supremo mandara que los ISP locales bloqueasen los sitios web de torrent, los sitios web de intercambio de archivos e incluso algunos sitios web de intercambio de vídeos, Anonymous tomó represalias doseando el Tribunal Supremo indio, el Ministerio de Comunicaciones y Tecnología de la Información, el Departamento de Telecomunicaciones, el Partido Bharatiya Janata y el Congreso Nacional indio. Al igual que muchos Anons, AnonOpsIndia recurrió a Twitter para hacer oír sus opiniones: «Nos convertiremos en un

#PAIN in the #ASS (grano en el culo) para el gobierno hasta que deje de #censurar nuestra #INTERNET[.] ¡NOS PERTENECE!»[300]

Anonymous siguió adelante con sus acciones en 2013, manteniendo el compromiso asumido con algunos asuntos en curso, como en el caso de #OpLastResort, una serie de hackeos retributivos lanzada contra los sitios web del Instituto Tecnológico de Massachusetts (MIT), el Departamento de Justicia de Estados Unidos y la Comisión Federal de Sentencias estadounidense, después del suicidio del pionero y activista de Internet Aaron Swartz. Su familia y muchos admiradores estaban convencidos de que su suicidio, a los 26 años, era un acto político provocado por la sensación de desesperación alimentada por su inminente juicio. Swartz se enfrentaba a treinta y cinco años de prisión y a 1 millón de dólares en multas, simplemente por haber descargado un caché de artículos para revistas académicas que nunca divulgó. «La muerte de Aaron... es el resultado de un sistema judicial penal caracterizado por la intimidación y la extralimitación procesal», escribieron su familia y su pareja.[301] En el vídeo que acompaña sus hackeos y desfiguraciones de sitios web, Anonymous reflejó este análisis:

> Hoy hace dos semanas se cruzó una línea roja. Hoy hace dos semanas murió Aaron Swartz. Murió porque se enfrentaba a una elección imposible. Murió porque le obligaron a participar en un juego que no podía ganar –una perversión retorcida y distorsionada de la justicia– un juego donde el único movimiento ganador era no jugar.[302]

Aunque inicialmente había recibido escasa atención por parte de los medios de comunicación, un trío de operaciones llevadas a cabo en Norteamérica centradas en una serie reciente de denuncias de agresión sexual y violación enganchó a los creadores de noticias estadounidenses. De pronto Anonymous volvía a ocupar el centro del escenario. De nuevo en su posición preferida, Anonymous consiguió estimular el debate público en torno a una cuestión tratada demasiado a menudo como un mero espectáculo goloso.

El primer caso, ocurrido en Steubenville, Ohio, tuvo como protagonistas a dos miembros de un equipo de fútbol americano de un instituto que se enfrentaban a juicio por haber violado a una compañera de

clase. La noche de la agresión, otros miembros del equipo sacaron fotos y filmaron a la chica inconsciente a causa del alcohol, compartiendo este material acto seguido en las redes sociales acompañadas de repugnantes comentarios jocosos. Uno de los vídeos, enviado finalmente a Anonymous, presentaba a uno de los compañeros de clase presumiendo de que «la violaron más duramente que ese poli que violó a Marcellus Wallace en *Pulp Fiction* [...] Así es como sabes que está muerta, porque alguien se mea encima de ella».[303]

En diciembre de 2012, mientras la activista Michelle McKee afirmaba que la celebración de un juicio justo era imposible en una ciudad que trataba a los jugadores de fútbol como si fueran semidioses, se puso en contacto con Anonymous y el colectivo intervino. Un Anon que recientemente había adoptado el apodo de "KYAnonymous" (su verdadero nombre es Deric Lostutter) se puso manos a la obra revelando las identidades de los pósters en foros de porno vengativo. Al leer sobre el caso de Steubenville, se indignó y lo expresó profusamente a través de Twitter. McKee le envió parte de un material incriminatorio que había circulado con cuentas de redes sociales de personas relacionadas con ese hecho. KYAnonymous pasó a la acción de inmediato lanzando en primer lugar un vídeo con una advertencia inquietante. David Kushner lo describió de manera memorable para la revista *Rolling Stone*:

> Como si fuese un jugador de póquer consumado, Lostutter subió la apuesta de su manifiesto con un farol. Afirmó que Anonymous ya había doxeado "a todos los implicados" en el encubrimiento y el delito –padres, profesores y chicos– y tenía intención de revelar su información privada en línea «a menos que todas las partes acusadas comparezcan el día de Año Nuevo y ofrezcan una disculpa pública a la chica y a su familia».[304]

Al día siguiente, un hacker llamado Noah McHugh, que se hacía llamar "BatCat", consiguió entrar supuestamente en RollRedRoll.com, el portal de la web deportiva del instituto (bautizada así por su mascota, un semental rojo brillante con aspecto de demonio) y accedió a los correos electrónicos del equipo de fútbol. KYAnonymous tuiteó sin parar mientras celebridades como Roseanne Barr añadían a la causa su efecto en la red. Luego, el 29 de

diciembre, un frío día invernal, la llamada de Anonymous a una manifestación callejera en Steubenville fue respondida por una multitud de un millar de participantes, con un despliegue de las ahora preceptivas máscaras de Guy Fawkes. «En un giro dramático, algunos de ellos hablaron de sus propios casos de agresiones sexuales y violaciones, quitándose las máscaras para mostrase ante la multitud», escribió Kushner.

Anonymous continuó implicado de manera hiperactiva a través de Twitter en el caso de la agresión de Steubenville, hasta que los dos adolescentes fueron declarados culpables de violación en marzo de 2013. Uno de los acusados recibió la pena mínima: un año en un centro correccional para menores. El otro acusado fue condenado a dos años. En noviembre de 2013, cuatro residentes de Steubenville, incluido el superintendente del instituto, fueron posteriormente acusados de encubrir pruebas de otro caso anterior de violación, según *The New York Times*.[305] El FBI registró el domicilio de Lostutter en junio de 2013 y se enfrenta a una acusación en el marco de la CFAA; Noah McHugh fue presuntamente arrestado en febrero. Si son condenados se enfrentan a penas de prisión mucho más largas que las de los violadores.

En abril de 2013, Anonymous se enteró del caso de Rehtaeh Parsons, una excelente estudiante que se había suicidado después de lo que parece haber sido una agresión sexual durante una fiesta donde corrió el alcohol en Halifax, Canadá. La imposibilidad de procesar a ninguno de los chicos acusados, afirmó Anonymous, se debió a la gestión deficiente del caso por parte de la Real Policía Montada de Canadá (RCMP). Anons ayudó a aumentar la sensibilización sobre el caso en la opinión pública a través de un vídeo y un comunicado de prensa exigiendo que la RCMP de Nueva Escocia emprendiera acciones legales de inmediato contra los individuos implicados. Leah Parsons, la madre de Rehtaeh, pidió que fuesen las autoridades las que hicieran justicia en lugar de los vigilantes en la red. Los Anons que estaban detrás de #OpJustice4Rehtaeh respetaron este deseo dejando claro en una declaración posterior que

> No aprobamos la justicia de los vigilantes, como afirman los medios de comunicación. Eso significaría aprobar acciones violentas contra estos violadores a manos de una multitud violenta. Lo que nosotros queremos es que se haga justicia. Y ese es vuestro trabajo. De modo

> que hacedlo. Los nombres de los violadores se reservarán hasta que sea evidente que no tenéis ninguna intención de hacer justicia para la familia de Retaeh. Por favor, tened en cuenta que hay otros grupos de Anons que también intentan revelar esta información y es posible que ellos no quieran esperar en absoluto. Será mejor que actuéis rápidamente.[306]

La RCMP reabrió el caso pero minimizó el papel de Anonymous, insistiendo en que las nuevas pruebas «no procedían de una fuente online».[307] Los participantes de Anonymous, junto con algunos comentaristas, pensaban que los activistas enmascarados habían marcado una diferencia decisiva: «Es absolutamente evidente que la presión ejercida en la red importó y mucho en este caso»,[308] observó Emily Bazelon, de *Slate*. Leah Parsons, que al principio había mostrado una actitud ambivalente, se mostró finalmente agradecida de que Anonymous hubiese intervenido en el caso. A finales de agosto de 2013, la RCMP imputó a los dos acusados de crear y distribuir pornografía infantil (el caso aún está pendiente).

El último de estos tres casos tuvo como escenario otro incidente que nunca llegó a juicio porque los fiscales consideraron que no había suficientes pruebas. Este caso tuvo por escenario una fiesta celebrada en Maryville, Missouri, después de la cual Matthew Barnett, de 17 años, echó de su casa a Daisy Coleman, de 14 años, apenas consciente, en camiseta y pantalones cortos, quien acabó desmayada y a temperaturas bajo cero. Dos exhaustivos artículos de investigación locales sugerían contundentemente que, de hecho, había pruebas más que suficientes para acusar a Barnett. Comparando esta situación con lo ocurrido en Steubenville, un artículo de Peggy Lowe y Monica Sandreckzi en *Kansas City Public Media* citaba al sheriff local: «¿Se cometió un delito? Joder, sí, se cometió. ¿Fue un delito horrible? Sí, fue un delito horrible. ¿Y deben ser castigados estos chicos por eso? Absolutamente.»[309] Cuando los artículos llegaron a oídos de Anonymous, el grupo agitó el avispero y llamó la atención de todo el país sobre este incidente. Finalmente, un fiscal especial presentó una denuncia formal contra Matthew Barnett por la comisión de un delito al poner en peligro a una menor de edad.

Las intervenciones de Anonymous en estos tres casos generaron

respuestas apasionadas pero divididas. Ciudadanos, periodistas y feministas discreparon sobre si las intervenciones de Anonymous habían ayudado o perjudicado a las víctimas de las agresiones sexuales. Ariel Levy, en un cáustico artículo publicado en *The New Yorker*, criticó con dureza a Anonymous (y a otros activistas en la red) al afirmar que el atractivo del grupo estaba arraigado en la ingenua adopción por parte del público de un simple arquetipo: «los Peter Parker de nuestros días, nerds informáticos que se ponen un disfraz y se transforman en superhéroes vigilantes».[310] Otras respuestas estaban más matizadas y trascendían el argumento de los vigilantes. Durante una videoentrevista en *Huffington Post Live*, la autora feminista Jaclyn Friedman reflexionó sobre la "espada de doble filo" del activismo en Internet:

> La víctima es victimizada una vez, pero vuelven a victimizarla cuando esos vídeos e imágenes circulan entre sus compañeros. Pero eso puede en algunos casos, como hemos visto en Steubenville –con la ayuda de Anonymous difundiendo esos vídeos– convertirse en una prueba, de modo que es más probable que se haga justicia.[311]

Anonymous encendió una conversación nacional desesperadamente necesaria sobre la cultura de la violación en Estados Unidos y Canadá. En un absorbente artículo publicado en *The New York Times Magazine*, Bazelon identificó un patrón en estas tres "operaciones de caballero blanco", un patrón que se aplica también a una muestra más amplia de las operaciones políticas ejecutadas por Anonymous, incluso aquellas que evitan el vigilantismo: cuando Anonymous sale a la palestra se debe habitualmente a la percepción por parte del grupo de que no se está haciendo justicia; en muchos casos esto resulta ser verdad.[312]En una entrevista de seguimiento que le hizo *The New York Times* sobre su investigación de Anonymous, Bazelon añadió,

> Creo que cada operación, u op, necesita ser juzgada individualmente. Unas operaciones que tienen a gente realmente responsable trabajando en ellas son probablemente en conjunto una cosa positiva. Creo que eso es así en el caso de Maryville y es probable que también en la operación de Rehtaeh Parsons, aunque esa es más tensa, porque estaba

acusada una persona inocente. Otras realmente descarrilan.

En efecto, Steubenville, el caso que concitó mayor atención de los medios de comunicación, fue en muchos aspectos la peor ejecutada de las tres operaciones. Entre otros problemas, la propia víctima fue doxeada por Anons y los vecinos del lugar fueron acosados. Muchos Anons estaban furiosos con Lostutter por haber lanzado el vídeo (y, una vez expuesto, la furia no hizo más que intensificarse cuando vieron que Lostutter se comportaba de una manera que muchos consideraron como de flagrante autopromoción).

Dos calificaciones merecen una reflexión adicional. Aunque la justicia de los grupos de vigilantes es justamente considerada problemática por eludir el proceso legal, aparece porque los canales actuales para ejercer justicia son débiles o inexistentes. Con demasiada frecuencia, los críticos señalan con el dedo a los "vigilantes", al tiempo que ignoran o minimizan las condiciones más sistémicas que, en muchos sentidos, originan su aparición. En segundo lugar, los equipos son capaces de adaptarse. He sido testigo de esta dinámica al menos una docena de veces; después de los errores que se cometieron en la operación Steubenville, las posteriores participaciones de Anonymous en casos de violación se abordaron con mayor delicadeza, supervisión y cuidado. Por supuesto, esa sensibilidad es en sí misma frágil; los grupos de trabajo dentro de Anonymous son propensos a la disolución. Podían funcionar bien de tres a seis meses y luego disolverse como consecuencia de niveles volcánicos de conflictos internos. (Bazelon describe con detalle las tormentosas discusiones que provocaron la disolución de uno de esos grupos.) Posteriormente podían reconstituirse con nuevos miembros que no habían interiorizado las mismas lecciones dolorosamente aprendidas.

A diferencia de otras iniciativas de otros hackers y geeks –como el caso de Debian, el mayor proyecto mundial de software– Anonymous no cuenta con una metodología establecida mediante la cual se pueda codificar a sí mismo como una institución. Solo existe un protocolo limitado –y provisional– para cumplir con los roles de adjudicación, reproducción social y asesoría. Por ejemplo, canales de IRC como #opnewblood, como su nombre sugiere, tienen fundamentalmente objetivos pedagógicos. Se trata de un espacio donde los recién llegados aprenderán los gajes técnicos y

culturales del oficio. Algunas cuentas de Twitter, como es el caso de @YourAnonNews –que en cierto momento tuvo más de veinticinco colaboradores a quienes se pedía que siguieran una guía de estilo– representan una mini organización mediática (@YourAnonNews ha sido criticada por algunos Anons como microimperialista).

Al hacer balance de la extensa constelación de prácticas que caracteriza a Anonymous, podemos obtener unas pocas y rápidas generalidades. Anons tiende a renunciar a los rígidos códigos normativos en favor de respuestas específicas, oportunas y basadas en hechos. Ellos luchan incluso con la memoria institucional, incluso cuando Anons o los medios de comunicación conmemoran las operaciones que se han llevado a cabo. Anonymous, no hay duda, exhibe una importante cohesión cultural, asegurada mediante todos los vídeos, memes y otras tradiciones culturales que produce el grupo. Pero, al mismo tiempo, Anonymous, o bien evita o nunca aplica políticas y mecanismos para manejar las operaciones. No se trata simplemente de que los Anons sean alérgicos a los formalismos. Considerando que cada operación es tan diferente de las demás, puede resultar muy difícil aplicar mejores prácticas en este medio dinámico, aun cuando podemos afirmar que Anonymous sin duda aprende del pasado.

Por supuesto, si todas las iniciativas de los activistas evitaran la institucionalización, serían sin duda los objetivos políticos más ambiciosos los que sufrirían las consecuencias. Pero la investigadora feminista Larisa Mann identifica los puntos fuertes de las iniciativas políticas flexibles, al sostener en una entrevista que «Anonymous podría estar por delante del feminismo dominante en la lucha contra la cultura de la violación en las localidades pequeñas».[313] Mann desarrolla el concepto: a diferencia de los actores institucionalizados, Anonymous (junto con otras formas efímeras de activismo desestabilizador) está libre de las ataduras de la “autopromoción y la financiación”, dos elementos que se exigen casi universalmente para llevar a cabo iniciativas institucionales. Estos requisitos pueden impedir la clase de respuesta rápida y hábil que Anonymous ha conseguido elevar a la categoría de arte.

Si hay alguna conclusión que se pueda extraer de una revisión superficial de estos casos, es ésta: la tarea de la transformación social y política requiere un juego de herramientas diverso, desde intervenciones gubernamentales afinadas hasta ruidosas tácticas subversivas. Deberíamos

ser precavidos a la hora de bautizar cualquier enfoque concreto como solución mágica. Si me viese obligada a elegir entre una ONG que trabaja por los derechos de la mujer y una intervención problemática e imprevisible de Anonymous, probablemente elegiría la primera. Pero esta dicotomía es como un hombre de paja. La cuestión urgente aquí es cómo promover la interdisciplinariedad. Es una actitud prudente que aquellos que están comprometidos con estos objetivos políticos pregunten cómo se pueden promover las alianzas, en lugar de criticarse por diferencias tácticas.

Necesitamos historias convincentes que den visibilidad a cuestiones que han sido descuidadas, tal como ha sostenido el experto en medios de comunicación y veterano activista Stephen Duncombe: él apoya totalmente la clase de espectáculo aportado por Anonymous y descartado con tanta ligereza como una fantasía juvenil masculina por periodistas como Levy.[314] Los grupos bien dotados de recursos, que cuentan con equipos especializados de abogados, promotores y estrategas políticos, que gestionan los recursos para destinarlos a intervenciones estratégicas y sostenibles a más largo plazo, son absolutamente necesarios. También necesitamos periodistas de investigación (bien pagados) que dediquen años a seguir la pista de las fuentes y reunir las piezas de complicados rompecabezas. Pero, como hemos podido ver en el caso de Maryville, estas estrategias, cuando se toman por sí solas y a falta de un recipiente agitado de dramatismo, a veces tristemente fracasan. Son incapaces de concitar la clase de atención o de voluntad colectiva necesarias para romper con esas prácticas y actitudes tan arraigadas. El auténtico problema reside en otra parte: muchas personas carecen de la voluntad, o bien son demasiado cínicas para, de entrada, entrar en la escena política y presentar batalla.

Conclusión

Aurora

El 6 de junio de 2013 me encontraba sentada en un frío auditorio de la Universidad de Nueva York mientras esperaba mi turno para intervenir en el Personal Democracy Forum (PDF), un acto anual que analiza el papel de Internet en la vida democrática. En aquellos días tenía la sensación de estar cayendo en un torbellino de negatividad. Escribir sobre quienes excavan, extraen y socavan, quienes desean resultar incomprensibles y permanecer ocultos y enigmáticos (parafraseo libremente las primeras líneas de *Aurora*, de Friedrich Nietzsche), me empezaba a parecer un ejercicio lleno de negatividad y pesimismo. Anonymous seguía levantando ampollas con sus operaciones políticas, pero Barrett Brown y Jeremy Hammond, y muchos otros hackers, estaban ahora en prisión. Internet se había convertido en una gigantesca y sofisticada máquina de seguimiento. Las empresas de defensa privadas, las grandes compañías como Facebook y las agencias estadounidenses de tres letras (junto a sus homólogas en Australia, Canadá, Nueva Zelanda y el Reino Unido) habían llevado a cabo un intenso trabajo: recogiendo cada huella, previendo cada uno de nuestros movimientos. Aunque cada organización y país lo hiciera con fines diferentes y empleara tácticas distintas, el efecto real había sido un recorte de los derechos preocupante y generalizado. Anonymous, pensaba sugerir en mi intervención, había sido «la parte ruidosa en el funeral de la libertad y la privacidad en la red».

No estaba sola defendiendo esta sombría evaluación. Como me había dicho en una ocasión un Anon, m0rpeth: «Cuando todo se haya perdido, nosotros seremos pequeñas redes oscuras dispersas en los confines de Internet.» Incluso los organizadores del PDF, habitualmente optimistas

acerca de la fuerza de Internet para decantar la balanza del poder en favor de la libertad y la justicia, habían reconocido durante una cena celebrada la noche anterior que «las cosas no han resultado como esperábamos».

Fue entonces, justo antes de que me llamasen al estrado, cuando Micah Sifry, el coorganizador del PDF, me lanzó un salvavidas de manera súbita e inesperada. Se inclinó, me alcanzó su teléfono y me susurró: «Ha habido una importante filtración sobre la vigilancia del gobierno.» Examiné superficialmente el artículo en la pantalla del teléfono. Con la firma del periodista Glenn Greenwald, el texto revelaba la impresionante colección de metadatos de registros telefónicos reunida por la compañía Verizon a instancias de la Agencia de Seguridad Nacional (NSA). En pocos días, Edward Snowden, el delator que había suministrado toda esa información, se convertiría en un nombre muy conocido. Sifry se dirigió al estrado para presentarme. Antes de hacerlo comunicó la noticia al público y alteró mi disertación sobre Anonymous para incluir este esperanzador giro de los acontecimientos.

La decisión de Snowden de dejar al descubierto a la NSA (y, por extensión, a su homólogo británico, el Cuartel General de Comunicaciones del Gobierno, el GCHQ) había sido un acto arriesgado pero cuidadosamente tramado. La acción de Snowden confirmaba lo que los activistas de la privacidad habían estado advirtiendo durante años, y les proporcionaba casos mucho más sólidos y amplios sobre los cuales basar sus alegaciones. Laura Poitras, una de los primeros tres periodistas que recibieron ese tesoro de documentos de la NSA, destacó la novedad de la situación: «Las revelaciones hechas por Snowden han corrido una cortina para dejar al descubierto un vasto mundo oculto donde se toman decisiones y el poder opera en secreto, al margen de cualquier supervisión o aprobación públicas. En realidad mi visión no ha cambiado, pero ahora ha aumentado considerablemente lo que puedo ver.»[315] He aquí apenas una fracción de lo que ahora podemos ver gracias a esta megafiltración: la NSA espió o vigiló directamente treinta y ocho embajadas y misiones; hasta 2011, la NSA recogió y almacenó enormes cantidades de correos electrónicos y metadatos de ciudadanos estadounidenses en el marco de un programa llamado Stellar Wind; la NSA obligó a los gigantes de la tecnología a entregar datos utilizando órdenes judiciales emitidas bajo el paraguas de la FISA (Ley de Vigilancia de la Inteligencia Extranjera), al tiempo que también accedía de

manera encubierta a los cables de fibra óptica, como los de Google, para desviar secretamente más datos todavía; la NSA hackeó los sistemas de comunicaciones internos de la cadena Al Jazeera; el GCHQ lanzó un ataque de DDoS contra Anonymous y hackeó Belgacom, una compañía de telecomunicaciones belga de propiedad semi pública; y bajo un programa acertadamente llamado Optic Nerve, el GCHQ interceptó y almacenó imágenes tomadas por cámara de millones de usuarios de Yahoo!. Y aún había más: una investigación llevada a cabo durante cuatro meses por Barton Gellman y Julie Tate demostró que «en las comunicaciones interceptadas por la Agencia Nacional de Seguridad, los usuarios corrientes de Internet, tanto estadounidenses como no estadounidenses, superan con creces a los extranjeros legalmente vigilados».316

Aunque parezca increíble, un informe de la NSA de 2012, incluido también entre los documentos filtrados, revelaba la insatisfacción de la agencia de espías con todos estos logros. La NSA pretendía ampliar aún más su alcance mediante el despliegue de una estrategia ciberofensiva incluso más agresiva, que les permitiese recopilar datos «de cualquiera, en cualquier momento, en cualquier lugar», según informaron Laura Poitras y James Risen para *The New York Times*.317

Esa clase de medios de vigilancia agresivos y de vasto alcance diezmaron preventivamente la posibilidad del "derecho a que te dejen en paz", por utilizar la famosa expresión de Samuel Warren y Louis Brandeis en 1890, que fueron de los primeros en considerar la base jurídica de la privacidad.318 Y el estilo de vigilancia empleado actualmente no ataca solo a la esfera privada, personal y académica que se considera valiosa en la formación liberal de la persona, sino que impide también muchas formas de asociación que son fundamentales para la vida democrática. Riseup, el colectivo de tecnología radical y proveedor de servicios de Internet, resume muy bien esta situación:

> La vigilancia es realmente, en su raíz, una forma muy eficaz de control social. Sabernos vigilados cambia nuestro comportamiento y reprime la disidencia. La incapacidad de asociarse secretamente significa que ya no existe ninguna posibilidad para la asociación libre. La incapacidad de susurrar significa que ya no existe ningún discurso verdaderamente libre de coerción, real o implícita. A niveles más

> profundos, la vigilancia generalizada amenaza con eliminar el elemento más vital tanto de la democracia como de los movimientos sociales: el espacio mental para que las personas construyan opiniones impopulares y discrepantes.[319]

Las agencias de inteligencia exigen naturalmente cierto secretismo para poder funcionar con eficacia por el interés público. Pero cuando el secretismo se priva de todo control —especialmente cuando se otorga a aquellas personas que ya disponen de cantidades extraordinarias de poder y de recursos— se convierte en un caldo de cultivo para la clase de abusos que vimos surgir bajo la dirección de J. Edgar Hoover en el FBI, tales como COINTELPRO, el programa de contrainteligencia cuyo objetivo era investigar y desbaratar a las organizaciones disidentes dentro de Estados Unidos.

El aparato de vigilancia expuesto por Snowden es también, tecnológicamente, y por lo tanto históricamente, singular. Si se dispone del poder informático suficiente, la recopilación de datos se vuelve terriblemente fácil, sobre todo mediante la automatización total. Y tal como señala la defensora de las libertades civiles Jennifer Granick, «una vez que has construido la trampa para ratones de la infraestructura de vigilancia, vendrán a por los datos».[320]

El Estado se apoya con especial fuerza en los datos recopilados y los informes de los soplones para apuntar activamente hacia grupos específicos; actualmente Estados Unidos y el Reino Unido espían de manera desproporcionada a musulmanes, activistas ecologistas y, cada vez más, a los hacktivistas.[321] Ésta es la conclusión a la que se ha llegado en *Mapping Muslims: NYPD Spying and Its Impact on American Muslims*, un informe de investigación sobre la expresivamente denominada Unidad de Demografía del Departamento de Policía de Nueva York, publicado por un trío de organizaciones sin afán de lucro.[322] Creado por un exoficial de la CIA poco después del 11/9, el programa demostró ser tan polémico e ineficaz –de los datos recogidos no se desprendió ninguna información de inteligencia fiable–, que fue eliminado en abril de 2014, pero solo después de que hubiese perturbado y distorsionado durante más de una década el tejido social de las comunidades musulmanas que habían estado en el punto de mira.[323] El programa incluía el empleo de 15.000 informantes y la

elaboración de un frondoso dosier mediante una exhaustiva vigilancia con vídeos y fotografías. Una estudiante universitaria musulmana incluida en el informe, Sari, sintetizó el carácter invasivo del programa en una sola frase: «Es como si la ley dijera: cuanto más musulmán eres, más problemático puedes ser, de modo que reduce tu islamidad.»[324] La filtración confirmó asimismo que la NSA vigila a "prominentes musulmanes estadounidenses", incluido abogados, profesores y otros profesionales, incluso cuando no tuvieran ningún vínculo con actividades terroristas o criminales. Después de tres meses de trabajo de investigación y entrevistas en profundidad con cinco objetivos, «todos ellos negaron tajantemente cualquier implicación en actividades de terrorismo o espionaje, y ninguno promueve la yihad violenta ni es conocido por haber estado implicado en ningún delito, a pesar de años de un intenso control por parte del gobierno y la prensa».[325]

En Estados Unidos, los musulmanes estadounidenses soportan el peso de lo que la ACLU describe como "vigilancia sin sospecha".[326] Pero el control omnipresente tiene consecuencias en la sociedad. Como ha argumentado de manera convincente la periodista Laurie Penny, «si vives en un estado de vigilancia durante el tiempo suficiente, acabas por crear un censor en tu cabeza».[327] Cuando las videocámaras son accesorios habituales en el paisaje urbano; cuando los gigantes corporativos de Internet almacenan registros de la comunicación y navegación online (y hacen que sea alarmantemente fácil que la NSA acceda a ellos); y cuando directores y jefes mantienen capacidades operativas para «juzgar y controlar a los empleados como nunca antes», en palabras del periodista Steve Lohr, la sociedad en su conjunto es la que paga el precio.[328] Estos diferentes vectores de vigilancia añadida ejercen presión para que nos integremos, para que pensemos dos veces antes de hablar, para que, en esencia, sigamos un estricto conjunto de normas prescritas. La conformidad social promueve la resignación pasiva y desincentiva los actos experimentales –y necesariamente arriesgados– de hablar, pensar y hacer que resulten fundamentales para una saludable discrepancia democrática.

¿Conseguiremos acaso nosotros, con la ayuda de personas como el excontratista de la NSA que asumió un riesgo tan enorme al hacer esas revelaciones, obligar a nuestros gobiernos a frenar esos abusos y, al hacerlo, recuperar así nuestro derecho a asociarnos libres de una vigilancia indebida? Los obstáculos son enormes; los canales autorizados para el

cambio político en Estados Unidos son terriblemente estrechos.[329] La arquitectura técnica de Internet, donde los servidores centralizados y controlados por las grandes corporaciones almacenan la mayoría de nuestros datos, hace que la captura sea a la vez ridículamente fácil y omnipresente. Este escenario técnico ha sido descrito por el abogado de las libertades civiles Eben Moglen como una "receta para el desastre", impulsándole a él y a otros tecnólogos de Internet, como el experto en seguridad Bruce Schneier, a declarar: «Necesitamos resolver de qué manera podemos rediseñar Internet para impedir esta clase de espionaje al por mayor.»[330] Por último, como sostiene el principal tecnólogo de la ACLU Chris Soghoian, mientras las empresas de Internet continúen «rentabilizando los datos privados de sus usuarios» nunca podrán adoptar una política de privacidad verdaderamente "pro usuario".[331]

Sin embargo, un terreno que parecía irremediablemente desierto, ahora parece un paisaje fértil. La familia geek políticamente comprometida continúa creciendo, tanto en tamaño como en importancia política. Está constituida por numerosas organizaciones y por una gran cantidad de activistas que trabajan con políticos, abogados, periodistas y artistas. Muchos surgieron de los cuarteles geek de Internet. Allí están Julian Assange, Birgitta Jónsdóttir, Chelsea Manning, Sarah Harrison, la Electronic Frontier Foundation, los desarrolladores de Tor, Anonymous, Riseup, Edward Snowden y muchos más. Los dos últimos años han tenido características singulares. Nunca antes tantos geeks y hackers habían puesto sus teclados al servicio de la libre expresión política, la disidencia y la acción directa.[332]

Cada vez más, gracias a sus acciones combinadas, somos capaces de reconocer que nos encontramos en una encrucijada. Snowden provocó un intenso debate nacional sobre la cuestión de la privacidad que se ha prolongado durante más de un año, un milagro menor en un panorama mediático masivo que celebra la novedad y evita el debate sostenido a largo plazo. Existen signos prometedores de cambios legislativos. En lo que el defensor de la libertad de expresión Trevor Timm describió como «una sorprendente amonestación a los abogados de la NSA y a la Casa Blanca», la Cámara de Representantes estadounidense aprobó en junio de 2014 un amplio proyecto de ley que prohíbe el acceso sin orden judicial a los correos electrónicos de los ciudadanos estadounidenses, y a las agencias de

inteligencia la instalación de puertas traseras en el hardware comercial, con o sin la complicidad del vendedor.[333] Los efectos de la filtración han reverberado a su vez mucho más allá de las fronteras nacionales, como confirma Glenn Greenwald:

> [La filtración de Snowden] cambió la manera en que la gente de todo el mundo veía la fiabilidad de cualesquiera declaraciones realizadas por funcionarios estadounidenses y cambió las relaciones entre los países. La filtración alteró radicalmente las concepciones sobre el papel correcto que debe cumplir el periodismo con respecto al poder del gobierno. Y dentro de Estados Unidos originó una coalición ideológicamente diversa, transpartidista, que presiona para conseguir una reforma significativa del estado de vigilancia.[334]

Todas estas consideraciones parecen incluso más destacables cuando se considera la perversidad con la que muchos funcionarios del gobierno, especialmente en la comunidad de inteligencia, han reaccionado ante el caso Snowden. Una anécdota es emblemática de esta actitud: durante la Conferencia sobre Defensa y Seguridad celebrada en Ottawa en 2014, Melissa Hathaway, exdirectora de la Joint Interagency Cyber Task Force (Fuerza Operativa Conjunta de Ciberseguridad Informática Interagencias) en la Oficina del Director Nacional de Inteligencia, relató a la audiencia que se había enterado del vuelo de Snowden a Rusia (en busca de asilo político) cuando se encontraba en Tel Aviv. «Debo decirles que los israelíes tenían un punto de vista que comparto. Que nunca se debió haber permitido que subiera a ese avión, y luego ellos [los israelíes] llevaron el asunto un poco más lejos: que el avión nunca tendría que haber aterrizado.» Cuando las carcajadas se apagaron, Hathaway puntuó ese sentimiento con una sola frase: «Aún podría suscribir ese punto de vista.»[335] No obstante, a pesar de que el estado norteamericano reduce la importancia de Snowden llamándole delincuente común, sus declaraciones políticas se vuelven cada día más destacadas. La propia Hathaway lo reconoció en la declaración que desencadenó la anécdota señalada más arriba. «Nuestros aliados se sienten traicionados. Sus ciudadanos creen que Edward Snowden es un héroe.»

Snowden había alimentado un incipiente movimiento integrado por colectivos de tecnologías, abogados, periodistas, cineastas, políticos y ONG

de diversas ramas. Este movimiento había prestado su voz a las luchas anteriores de grupos como las organizaciones sin afán de lucro Fight for the Future y Open Technology Institute. El resultado ha sido un conjunto de campañas políticas y tecnológicas específicas, tales como Reset the Net, una iniciativa de base para «difundir las herramientas de privacidad de resistencia a la NSA» de modo que pudiesen convertirse por defecto en funciones de Internet.[336] Tecnologías como The Amnesic Incognito Live System (conocido también como Tails, un sistema operativo creado para el anonimato), Open Whisper Systems (una iniciativa de fuente abierta para desarrollar software de encriptación para teléfonos móviles) y LEAP (un acrónimo recursivo para el LEAP Encryption Access Project, que modifica las herramientas de encriptación existentes para volverlas fáciles de usar) están siendo financiadas por ciudadanos y organizaciones como la Freedom of the Press Foundation. El propio Snowden ha avalado proyectos de encriptación como herramientas eficaces y necesarias: «La conclusión es que la encriptación funciona», dijo en marzo de 2014 dirigiéndose a un auditorio donde no cabía un alfiler en South by Southwest (evento que se celebra cada primavera en Austin, Texas, y congrega seminarios y conferencias sobre películas, música y medios interactivos).[337] Estas tecnologías están preparadas para facilitar una cierta privacidad a las futuras generaciones de usuarios de Internet.

VIEJO MUNDO VERSUS NUEVO MUNDO

Poco después de la primera tanda de revelaciones de la NSA, Irlanda vio su primer caso judicial relacionado con actividades de hackeo. Dos miembros de LulzSec y Anonymous, Donncha O'Cearbhaill y Darren Martyn, fueron juzgados en julio de 2013 por la desfiguración del sitio web del partido político irlandés Fine Gael. Cuando me dirigía al juzgado en Dublín me perdí y llegué tarde. Como no llevaba ningún dispositivo de localización personal (o teléfono móvil) hice lo que la gente ha hecho durante siglos: consulté un mapa de papel y me confundí todavía más. Me llevó otros cuarenta y cinco minutos llegar al juzgado correcto, situado en un moderno edificio redondo de cristal. Estaba convencida de que me había perdido los procedimientos.

Resultó que los dos casos estaban intercalados entre más de una docena de audiencias por delitos menores; pasaría otra hora antes de que O'Cearbhaill y Martyn se presentaran ante el juez. Mientras esperaba, sentada junto a un Anon local apodado Firefly, nos lo pasamos en grande observando a la juez –una mujer razonable y con aspecto de matrona que rondaba los 50 años– mientras regañaba amablemente, pero con firmeza, a la docena de otros acusados. La mayoría de ellos habían estado implicados en travesuras juveniles y comportamiento violento. En un caso, una chica de veintipocos años con una cabellera negra increíblemente larga, el ceño fruncido de indignación, los brazos cruzados sobre el pecho y una vestimenta nada recatada fue declarada culpable de golpear a un agente del Garda –la policía local– estando completamente ebria.

Los dos casos de Anonymous se destacaban claramente de la serie de peleas y travesuras de borrachos. Tras escuchar a ambas partes en los dos casos de desfiguración, la juez mostró su escepticismo ante la afirmación hecha por el fiscal de que recuperar el sitio web del Fine Gael era un procedimiento caro. ¿Cómo podría costar diez mil euros, preguntó, si no había sufrido ningún daño? El fiscal no tenía ninguna respuesta. La juez concluyó que este hackeo era una «maniobra para avergonzar a un partido político más que para revelar datos al público en general». Ella no quería que O'Cearbhaill y Martyn acabasen a la cárcel por el equivalente digital a pintar graffiti. Pero tampoco pensaba que sus actos fuesen loables. En cambio, les amonestó a ambos, describiendo su hackeo como un "terrible abuso de talento". Luego les aplicó una multa de cinco mil euros a cada uno, pagaderos en octubre (y con la mitad de esa suma destinada a organizaciones benéficas) y ordenó que ingresaran en un programa de justicia restitutiva. No consideró que su acción tuviese una motivación política; si lo hubiese considerado bajo esa perspectiva, la pena podría haber sido un castigo incluso más leve.

Una vez levantada la sesión, O'Cearbhaill y Martyn se marcharon con sus familias. Firefly y yo nos dirigimos al centro de la ciudad caminando bajo el sol a lo largo del canal principal de Dublín. Irlanda estaba bajo una milagrosa ola de calor de dos semanas. Juntos analizamos detalladamente el juicio. Coincidimos en que O'Cearbhaill y Martyn habían salido bien parados; comparado con los Anons juzgados en Estados Unidos, las penas impuestas a los irlandeses y británicos eran notablemente leves. Si bien el

acto de desfigurar un sitio web no se puede comparar con las acciones cometidas por Hammond, la larga cadena de hackeos que Ryan “Kayla” Ackroyd, un ciudadano británico, llevó a cabo con LulzSec se acerca un poco más. En mayo de 2013, después de declararse culpable de un cargo de hackeo del Pentágono y de conspirar para hackear a Sony, el Servicio Nacional de Salud británico y la empresa News International de Rupert Murdoch, el Estado británico condenó a Ackroyd a treinta meses de cárcel, de los que cumplió diez; cabe mencionar que no se le impuso ninguna multa. En los casos sustanciados en Estados Unidos, incluso cuando las penas de prisión son relativamente cortas, las multas añadidas condenan virtualmente a años de servidumbre por deudas. A los 32 años, John Anthony Borell III, alias *Kahuna* de los CabinCr3w, fue condenado a treinta y seis meses de prisión por el hackeo de múltiples sitios web de la policía y descarga de datos personales. Una vez cumplida la condena, Kahuna todavía deberá pagar casi 230.000 dólares en concepto de daños.

Además, muchos de los cargos presentados contra hackers en Estados Unidos parecen haberse originado en el sector de la izquierda, como lo demuestra el calvario sufrido por Barrett Brown. El 6 de marzo de 2012, el mismo día en que Fox News expuso a Sabu y el FBI arrestó a Hammond, los agentes del gobierno ejecutaron una orden de registro en la residencia de Barrett Brown. Entre otras cosas, las autoridades procuraban localizar «registros relacionados con HBGary, Infragard, Endgame Systems, Anonymous, LulzSec, IRC Chats, Twitter, wiki.echelon2.org y pastebin.com».[338] Seis meses más tarde, en septiembre, el FBI arrestó a Brown (en vivo durante una videoconferencia, apropiadamente) después de que él –seamos francos– lo pusiera muy fácil para una redada. Brown había colgado en la red un vídeo titulado “Por qué pienso destruir al agente del FBI Robert Smith. Tercera parte: La venganza de los Lithe”, donde realizaba una arenga exagerada contra un agente federal que había interrogado a su madre.[339] Como era previsible, Brown fue arrestado por amenazas contra un agente del FBI. Un extracto de la diatriba de Brown demostrará con mayor claridad por qué estaba tan furioso, y por qué el FBI, a su vez, se había visto obligado a registrar su casa (en lugar de desechar simplemente el vídeo como una pieza de arte en vivo):

Adivinad lo que dice mi puta orden de registro: ¡fraude! No tengo un

> centavo [...] una puta acusación de fraude contra un puto activista escritor, que no tiene pasta, que ha gastado todo su dinero en putos abogados para él y su puta madre... El agente Smith publicó las direcciones de [mi casa y la casa de mi madre] Es un delincuente, implicado en una conspiración criminal... En cualquier caso, ésa es la razón por la que Smith está acabado. Cuando digo que está acabado, no estoy diciendo que voy a matarle, pero voy a arruinar su vida y a vigilar a sus putos hijos... ¿Le gustan las manzanas? Tal como Smith ha señalado, corro peligro por los Zetas ... Gracias por eso, tío [por revelar mi dirección] ... Voy a suponer que, como los Zetas adoptan a menudo la apariencia de personal de seguridad mexicano [y a menudo son] oficiales del gobierno, me preocupa que aquí se haya practicado el mismo truco... Especialmente el FBI ... serán considerados como potenciales escuadrones de la muerte de los Zetas, y como el FBI [sabe] ... saben que estoy armado, que vengo de una familia de militares, que un veterano de Vietnam me enseñó a disparar... y les dispararé a todos ellos y les mataré si vienen y hacen cualquier cosa, porque están involucrados en una conspiración criminal y tengo razones para temer por mi vida no solo por los Zetas, sino por los gobiernos estadounidenses [sic]... No tengo más opción que defenderme a mí mismo, a mi familia... y francamente, sabéis, era bastante obvio que iba a morir antes de los cuarenta, de modo que no me importaría irme con dos pistolas del FBI como un puto faraón egipcio. Adiós [en español en el original].

Junto a los cargos presentados a raíz de estas amenazas, Brown también se enfrentaba a cargos relacionados con el hackeo a Stratfor. En su sala de chat del Proyecto PM, Brown había compartido un enlace de red a un archivo alojado externamente que contenía los datos filtrados de las tarjetas de crédito de Stratfor. Por esa acción fue acusado de diez delitos de suplantación de identidad con agravantes y dos delitos relacionados con fraude con tarjetas de crédito, con una posible condena combinada total de cuarenta y cinco años (más los sesenta y pico de años por los otros cargos). Muchas otras personas que han hecho circular públicamente el enlace no fueron acusadas de ningún delito. El periodista Adrian Chen, que tendía a mostrarse crítico con las actividades de Anonymous, escribió: «Como

periodista que cubre a los hackers y ha “transferido y posteado” muchos enlaces a datos robados por hackers –con el fin de incluirlos en noticias sobre los hackeos— esta acusación me resulta inquietante porque parece criminalizar los enlaces.»[340]

Brown era una figura ambigua porque desempeñaba el papel ético de Anonymous y se presentaba como el rostro de un colectivo que procuraba no tener rostro. Sin embargo, Anons coincidió con Kevin Gallagher, el administrador de sistemas que dirige la campaña de apoyo a Brown, cuando sostuvo que «fue este trabajo periodístico de investigar en áreas que las personas poderosas preferirían mantener en la oscuridad lo que le convirtió en un objetivo».[341] Los simpatizantes de Brown recaudaron fondos, ayudaron a conseguir abogados de alto nivel y trabajaron para politizar los cargos presentados contra él.

En una sorprendente vuelta de tuerca, el gobierno retiró los cargos relacionados con el enlace solo dos días después de que la defensa presentara una moción para desestimar los cargos. (Retirar los cargos evita los malos precedentes y permite que el gobierno prosiga las investigaciones de la misma naturaleza.) Expuesto todavía a décadas de cárcel, con la prohibición de hablar con los medios de comunicación y habiendo pasado ya más de año y medio en prisión preventiva, un mes más tarde, en abril de 2014, Brown aceptó un acuerdo de culpabilidad. El acuerdo reducía drásticamente la sentencia potencial a alrededor de ocho años, y Brown se declaró culpable de solo tres delitos: ser cómplice después de cometido el hecho (en el hackeo de Stratfor), obstrucción a una orden de registro de ordenadores portátiles escondidos debajo del fregadero de la cocina y amenazas contra el agente del FBI.

La moraleja es la siguiente: ya sea que uno pretenda hackear con impunidad y anonimato –por motivos políticos o no– o simplemente para conseguir el estatus de agitador ingenioso, es mejor hacerlo en el lado europeo del Atlántico (donde Anonymous y otras formas de activismo geek son más comunes).

Más tarde, al anochecer en Irlanda, intenté preguntarle a O’Cearbhaill qué pensaba sobre el caso, pero no pude encontrarle en ninguna parte. Resultó que agentes del Garda le habían estado esperando fuera del juzgado, donde volvieron a arrestarle, esta vez no por sus actividades como hacker. O’Cearbhaill, estudiante de química, tenía un laboratorio en casa de

sus padres. Algunos de los productos químicos encontrados allí podían utilizarse (en teoría) para fabricar explosivos. Aunque no había absolutamente ninguna prueba de que O'Cearbhaill estuviera utilizando, o tuviese intención de utilizar, los productos químicos para dicho propósito, fue arrestado bajo la legislación antiterrorista irlandesa.

Aunque posteriormente el fiscal determinó que no había pruebas suficientes para presentar cargos, algunos Anons plantearon la hipótesis de que la Garda intentaba intimidar a O'Cearbhaill para que confesara su supuesta implicación en lo que se ha convertido en un hackeo legendario. A comienzos de febrero de 2012, AntiSec había publicado un archivo de audio de una teleconferencia interceptada entre el FBI, Scotland Yard y la Garda. El tema de la llamada telefónica no era otro que el propio Anonymous. La llamada filtrada no fue solamente un hackeo cien por cien lulz, sino también un (aparentemente) duradero ridículo para las agencias implicadas, en particular la Garda. La cuenta de correo electrónico de uno de sus propios oficiales había sido la pieza comprometida para obtener los datos necesarios para "unirse" a la llamada. (En el momento de escribir este texto, todavía nadie ha sido encontrado culpable de esta intrusión.)

El caso también puede sugerir otra razón de por qué las fuerzas del orden se muestran tan hostiles hacia los espeleólogos informáticos. En ocasiones, los hackers se imponen la misión de "vigilar a los que vigilan". Dos Kevin –Poulsen y Mitnick– lo habían hecho antes. El experto en medios de comunicación Douglas Thomas, que cubrió el calvario sufrido por ambos hackers, observó cómo «Poulsen hackeó los sistemas del FBI y descubrió un laberinto de escuchas ilegales y programas de vigilancia que controlaban a todos y todo, desde el restaurante situado al otro lado de la calle hasta (supuestamente) a Ferdinand Marcos».[342] AntiSec reveló lo mismo, solo que de forma todavía más ruidosa y pública.

Unos días más tarde, O'Cearbhaill, nuevamente en libertad, se unió a un grupo que disfrutábamos de un picnic de verano en Saint Stephen's Green. Yo había conseguido reunir a una representación de Anons procedentes de diferentes redes y objetivos operativos, desde el excienciólgo Pete Griffiths (un agudo partidario de Anonymous) hasta David de Chanology, Firefly de AnonOps y hackers como O'Cearbhaill. O'Cearbhaill me contó más cosas sobre cómo se había metido en el hacktivismo a los 15 años y sobre las experiencias de su padre en el IRA,

incluidos los seis años que pasó en la cárcel y la huelga de hambre de cuarenta días en la que participó. Su padre, a diferencia de la juez, había entendido naturalmente que las acciones cometidas por su hijo tenían una motivación política. Hacia el verano de 2013 ya estaba convencida de que la mayoría de los participantes de Anonymous tenía una inclinación política; con sus acciones podían excavar y debilitar, pero lo hacían hasta la llegada de la aurora, para acabar con el reino oscuro de la injusticia. Aun así, alguna cosa cambia cuando una persona escucha historias como las que O'Cearbhaill compartió conmigo. Las sombras y percepciones fugaces se vuelven sólidas y legibles; se hace evidente que cada contribuyente tiene una rica historia que le ha llevado hasta Anonymous y que el propio Anonymous funciona a modo de portal para poder llegar a más destinos.

De hecho, un año más tarde regresé a Dublín y, junto a otros cincuenta miembros del público, me instalé en la Science Gallery del Trinity College y escuché a O'Cearbhaill –ahora auditor del Partido Pirata de la Universidad de Dublín– dar una charla sobre Tor, la herramienta de privacidad. Estábamos en una reunión organizadas por CryptoParty, un movimiento de base cuyo propósito es enseñar criptografía al público en general. La idea había sido articulada por Asher Wolf y algunos otros geeks en 2012. Unos días más tarde, tomando unas cervezas en un pub de Londres, Mustafa Al-Bassam (tflow) me habló acerca de sus prácticas en Privacy International, la principal ONG europea de lucha por el derecho a la privacidad. Hay docenas de otros ejemplos. Cualquiera que sea la opinión que uno tenga de Anonymous, estaba claro que el colectivo actuaba como un portal político. Muchos de los que abandonaron el grupo continuarán contribuyendo a la vida política por diferentes medios.

A diferencia de Al-Bassam y muchos otros, Hammond y Monsegur eran activistas mucho antes de que se implicaran en las actividades de Anonymous. Pero sus caminos se separaron radicalmente cuando acabó su participación con el colectivo. Poco después de aparecer la noticia sobre su cooperación con las autoridades, Monsegur desapareció y nadie tenía idea de dónde se había metido. Resultó que había pasado un poco más de siete meses en el Metropolitan Correctional Center, la misma prisión donde había estado encarcelado Hammond antes de que lo trasladasen a Kentucky para cumplir su condena de diez años. Una fuente anónima me había pasado ese dato, pero mis súplicas a los periodistas para llevar a cabo una investigación

más detallada sobre por qué estaba en prisión cayeron en oídos sordos. Solo un tiempo después recibí la confirmación del propio Hammond. No fue hasta el 26 de mayo de 2014, cuando Monsegur fue finalmente condenado después de siete aplazamientos, que las circunstancias que llevaron al arresto y el encarcelamiento de Monsegur se hicieron públicas. Había violado las condiciones de su libertad bajo fianza redactando un post en un blog y chateando con un participante de Anonymous. En la audiencia para dictar sentencia, la juez Loretta Preska calificó a Monsegur de informador modélico y dictaminó que su estancia en prisión en 2012 era castigo suficiente. Era un hombre libre. Antes de abandonar el tribunal, Preska volvió a elogiar a Monsegur: «La inmediatez de la cooperación del señor Monsegur y la naturaleza permanente de la misma resultaron especialmente útiles para el gobierno... Esa característica personal de dar un giro a su vida para hacer el bien, no el mal, es el factor más importante en esta sentencia.» La sentencia indulgente de Preska trasmitía de manera no muy sutil el siguiente mensaje a los futuros informadores: cooperad y seréis bien tratados.

Aunque el resultado distaba mucho de ser sorprendente, Twitter se llenó de lamentos indignados: «Jeremy Hammond está cumpliendo una condena a diez años por hackeos que Sabu (trabajando para los federales) le dijo que cometiera. ¿Cuándo irán a prisión los federales?»[343] preguntó @YourAnonNews. «Preska es una absoluta desgracia para el concepto de justicia», manifestó Firefly durante una entrevista. Estas quejas no pudieron hacer nada para cambiar la situación de Hammond, pero muchos Anons obtuvieron cierta satisfacción cuando, apenas unos días después, tanto *Motherboard* como el *Daily Dot* publicaron sendos artículos que ponían en tela de juicio el argumento presentado por el gobierno, corroborando efectivamente la versión de los hechos ofrecida por Hammond. Junto con la colaboración “permanente”, las noticias constataban que Monsegur había dispuesto de libertad total para iniciar y coordinar docenas de hackeos.

Después de la puesta en libertad de Monsegur, Hammond publicó su propia declaración: «Mediante la persecución agresiva de los hackers que juegan según sus propias reglas, quieren impedir que otros se sumen a la causa y esperan que los futuros arrestos produzcan más cooperadores ambiciosos. Debemos continuar rechazando las excusas y justificaciones que consideran aceptable vender a tus amigos y convertirte en un peón del

ciberimperialismo... Sabu esquivó la condena a prisión, pero las consecuencias de sus acciones le perseguirán durante toda su vida. No habiendo cumplido siquiera la mitad de mi condena, seguiré estado donde estoy: aunque puedan quitarte temporalmente la libertad, tu honor dura para siempre.»[344] Si bien la prolongada detención de Hammond será indudablemente dura, su compromiso manifiesto con sus principios a pesar de su desenmascaramiento y encarcelamiento ya han demostrado ser un faro de inspiración para muchos en la comunidad de activistas.

Aunque pudiera parecer inusual que un investigador se comprometa tanto con el objeto de su estudio, ha sido durante mucho tiempo una nota predominante para el curso de antropología. Como escribe Danilyn Rutherford, los métodos antropológicos «crean obligaciones, obligaciones que obligan a aquellos que buscan el conocimiento a arriesgarse a hacer declaraciones verdaderas que saben que influirán en el entorno y en las personas que describen».[345] Como parte de una campaña de correo organizada por los abogados de Hammond, junto con otros 150 ciudadanos le escribimos a la juez Loretta Preska para pedirle indulgencia; en las cartas subrayábamos la naturaleza política de Anonymous. Siempre que ha sido posible he tratado de traducir el desconcertante mundo de Anonymous para diferentes públicos. También he escrito cartas a algunos de los Anons en prisión. Como parte de estas obligaciones, he reflexionado mucho y expresamente acerca de los objetivos subyacentes que motivan este libro. Finalmente llegué a la conclusión de que me impulsan dos objetivos contrapuestos: erradicar la desinformación y adoptar el hechizo.

En primer lugar, en este libro he buscado disipar algunos de los muchos conceptos erróneos que circulan con respecto a Anonymous: a muchos participantes como O'Cearbhaill no los guiaba principalmente un deseo de acumular lulz, si bien este espíritu irreverente aún regía las intervenciones sociales y suscribía las estrategias. Anonymous ha madurado hasta convertirse en un movimiento político serio, hasta el extremo de que muchos de los trols que actuaban en la época de La máquina del odio de Internet «no reconocerían al Anonymous de hoy», como me dijo Ryan Ackroyd. Ryan se encuentra dentro de esa diminuta porción de participantes que salvó la divisoria entre estas etapas hoy claramente distintivas. (Esto, naturalmente, no significa que La máquina del odio de Internet no vuelva a ponerse en marcha, como tuiteó un activista de Anonymous llamado

“blackplans”: «Sin los trols, los hackers, las hordas de 4chan, ¿cuántos de vosotros, personas agradables y sensibles, hubiérais oído hablar nunca de #Anonymous? No lo olvidéis».)[346]

Como parte de esta primera misión, he intentado evitar la exaltación de cada movimiento realizado por Anonymous. Incluso en sus avatares activistas, Anonymous ha participado claramente en acciones moralmente turbias y, en ocasiones, directamente horribles. Los momentos más preocupantes se producen cuando gente inocente se ve sorprendida en medio del fuego cruzado de Anonymous. Algunas operaciones de hackeo me parecieron contraproducentes, y no siempre merecieron la pena los riesgos que corrieron las personas implicadas. De hecho, algunas partes de Anonymous están plagadas de contradicciones irresolubles.

Y así, cuando se evalúa a Anonymous, parece imposible alcanzar una máxima universal —mucho menos limpia y ordenada— con respecto a los efectos provocados por el grupo. En cambio, he intentado transmitir las lecciones de Anonymous a través de la narración de sus gestas, fracasos y éxitos. Estas historias recopiladas son idiosincráticas y están contadas desde la perspectiva de mis viajes y anhelos. Hay tantas historias secretas y nunca contadas que, si se hicieran públicas, probablemente cambiarían nuestra comprensión de Anonymous. Si bien la vida social y los movimientos políticos son complejos, incluso intrincados, con facetas y dimensiones infinitas, la adopción por parte de Anonymous de la multiplicidad, el secretismo y el engaño contribuye a que sea especialmente difícil estudiarlo y entenderlo.

Este dinamismo y esta cualidad multitudinaria constituyen también uno de los principales puntos fuertes de Anonymous. Anonymous es un colectivo emblemático de una particular geografía de la resistencia. Compuesto de numerosos grupos que compiten entre sí, el poder a corto plazo se puede conseguir durante lapsos breves, mientras que el dominio a largo plazo por un único grupo o persona es virtualmente imposible. En un panorama tan dinámico puede resultar «fácil cooptar, pero imposible mantener la cooptación», como lo describió Quinn Norton reflexivamente durante su participación en un panel de South by Southwest, en marzo de 2013. De esta manera, la “naturaleza” multitudinaria de Anonymous impide su sometimiento tanto a figuras ambiciosas que trabajan internamente como a figuras externas que pudieran ejercer su influencia mediante

informadores, como Sabu, o a través de una presión exógena al grupo. Anonymous es un colectivo críptico que nos obliga a trabajar y bailar con los restos y fragmentos que nos muestra.

Es decir, Anonymous deja mucho a la imaginación. Pero no todo; es fundamental entender de qué modo Anonymous experimentó una metamorfosis desde los trols del submundo hasta los activistas cara al público, sobre todo si tenemos en cuenta que a Estados-nación, fiscales, funcionarios del gobierno y jueces les encantaría expulsarles a todos como simples delincuentes. Estos poderes fácticos no están dispuestos a reconocer que las acciones protagonizadas por Anonymous están generadas por una vocación activista; de hecho, pueden ser la potencia y el carácter motivado políticamente que caracterizan las acciones del grupo las que impulsan al Estado a criminalizarles con tanta rapidez.[347]

Y entonces, si bien me había propuesto eliminar los conceptos erróneos, la posibilidad de eliminar el aura de magia y misterio parecía de alguna manera inaceptable (en caso de que fuese siquiera posible). La filósofa Jane Bennett hace un llamamiento a que «nos resistamos a la historia del desencanto de la modernidad» y, en cambio, a «aumentar el hechizo».[348] Este ha sido mi segundo objetivo al recopilar historias fascinantes sobre Anonymous. Esta elevación deliberada del hechizo, sostiene Bennett, es un gesto político significativo y uno que estoy dispuesta a hacer por razones que se volverán más claras en estas últimas páginas.

Dado este segundo objetivo, era natural para mí adoptar un marco mítico e invitar al embaucador a que hiciera el viaje conmigo. Las figuras que aparecen en este libro representan las contradicciones y paradojas de la vida, muchas de las cuales son irresolubles. Al referir las historias de estos personajes surgen lecciones, no a través de secas descripciones sino a través de fascinantes, a menudo osadas, narraciones de proezas. La tradición del embaucador puede ser notablemente mítica, pero conviene recordar que, en un momento determinado de la historia, fue hilada por manos humanas. Mi función ha sido la de hacer avanzar este proceso de construcción histórica y política del mito, ya evidente en el funcionamiento rutinario de una entidad constituida por artistas expertos, creadores de mitos contemporáneos e inventores de fantasías.

Ahora que casi hemos llegado al final de este viaje y he desvelado los

objetivos que guiaron mi libro, el lector es quien ahora debe juzgar si he exhibido el ingenioso requisito necesario para equilibrar las fuerzas apolíneas del empirismo y la lógica con las fuerzas dionisíacas del encantamiento. Cualquiera que sea tu conclusión, permíteme la licencia de tejer algunos pensamientos finales a través y a lo largo de las lagunas que aún persisten y encima de otras áreas ya recubiertas de bordados. Mientras Anonymous a menudo me sigue dejando desconcertada, hay un hilo de mensajes inspiradores que podemos recoger en su estela.

Anonymous en todas partes

Aunque se trata de un colectivo inestable, y aunque sus estructuras organizativas nunca pueden ser comprendidas del todo, Anonymous está compuesto de personas que deciden juntas y por separado tomar cartas en el asunto. ¿Quién podría ser esta gente? ¿Un vecino? ¿Una hija? ¿Una secretaria? ¿Un conserje? ¿Un estudiante? ¿Un budista? ¿Un banquero de incógnito? ¿Tú? Cualquiera que sea la clase de gente que forma parte hoy del colectivo, una cosa es cierta: lo que comenzó como una red de trols se ha convertido en un manantial de insurgencia online. Lo que se inició como una reducida reacción contra la Iglesia de la Cienciología hoy comprende una selección mundial de causas políticas, desde luchas contra la censura en Túnez hasta salvas contra la cultura de la violación en Estados Unidos y Canadá y condenas a las injusticias económicas y políticas expresadas en Zuccotti Park y en la plaza Tahrir.

A pesar de una actitud frente a la ley imprevisible, por no decir irreverente y a menudo destructiva, Anonymous ofrece también una lección objetiva de lo que Ernst Bloch, el filósofo de la Escuela de Frankfurt, llama “el principio esperanza”. Bloch, que tuvo que huir de la Alemania nazi, escribió un tratado en tres volúmenes sobre esta cuestión durante su exilio en Estados Unidos. En busca de una explicación “enciclopédica”, Bloch descubrió una cantidad de signos, símbolos y artefactos asombrosamente diversos utilizados para encauzar la esperanza en diferentes épocas históricas. Los ejemplos reunidos incluyen desde ensoñaciones personales hasta cuentos de hadas consagrados por el tiempo, desde el amor por la música y los deportes hasta los tratados filosóficos o místicos, cualquier

cosa que pudiese encender o comunicar un rayo de esperanza. Trabajando a la sombra de una excesiva tensión de crítica marxista, su obra nos recuerda que un mundo mejor —o al menos la comprensión de lo que podría ser ese mundo— está entre nosotros. Como una suerte de arqueólogo filósofo, Bloch excavó mensajes de utopía ocultos u olvidados que podían combatir la "ansiedad" y el "miedo" en todos aquellos que los encontrasen. «La emoción de la esperanza sale fuera de sí, libera a las personas en lugar de confinarlas», escribe Bloch. «El trabajo de esta emoción requiere de personas que se lancen activamente a aquello en lo que se están transformando, a lo que ellas mismas pertenecen.»[349] El hecho de que una sólida política del activismo surgiese de las profundidades de uno de los lugares más sórdidos de Internet, de que los geeks eligiesen lanzarse activamente a un proceso de transformación política, me parece una representación perfecta de ese principio de esperanza.

Bloch acusaba a la "esperanza fraudulenta",[350] que se caracteriza por un optimismo ciego o manifiesto, por su fracaso en catalizar el movimiento. En cambio, su esperanza es incansable, sustentada por la pasión, el asombro e incluso la travesura, cualidades todas ellas adoptadas por Anonymous. Podemos ver entonces un sólido positivismo inherente en Anonymous, un empeño orientado hacia una forma realista de esperanza que, una vez explicitada, parece idónea para impulsar la ruptura y el cambio. Estas actividades, naturalmente, no ejercen ningún monopolio sobre los estados afectivos de la pasión y la esperanza. No obstante, con la excepción de un grupo restringido de pensadores importantes como Chantal Mouffe y Jacques Rancière, el carácter emocional de la vida política se ve a menudo relegado a los márgenes, un fenómeno extraño porque el deseo y el placer son esenciales a su ser mismo. Pero existen otras razones, más apremiantes que simplemente anular la omisión de un componente primordial de las iniciativas activistas, para transmitir los factores emocionales que cumplen un papel integral en el cambio social.

En 2008, cuando la temible y "Lokiana" banda de trols que entonces constituía Anonymous tomó un decisivo giro a la izquierda alejándose de las "cabronadas ultracoordinadas" y acercándose al activismo, conquistaron uno de los sentimientos predominantes de nuestro tiempo. Whitney Phillips, el experto en medios de comunicación, sostiene de forma convincente que nuestro momento está impregnado por un extendido cinismo, y que en los

trols encontramos uno de los extremos más destilados, concentrados y grotescos de una subcultura emocionalmente disociativa (o políticamente fetichista).[351]

Muchos teóricos y escritores pertenecientes a tradiciones radicalmente distintas, que van desde el novelista estadounidense David Foster Wallace hasta el autonomista italiano Franco "Bifo" Berardi, han argumentado persuasivamente que el cinismo se ha convertido en un prisma a través del cual amplios grupos de norteamericanos y europeos filtran y sienten el mundo. Wallace escribe acerca de la omnipresencia del «malestar y el cinismo pasivos» y hace un llamamiento para que «los antirrebeldes, espectadores natos se levanten y se atrevan de alguna manera a alejarse de la observación irónica».[352] Bifo, que ha escrito numerosos tratados sobre este tema, se vuelve hacia la poesía para transmitir la alarmante y muerta carga emocional de cinismo:

> Antes de que golpee el tsunami, ¿sabes cómo es?
>
> El mar retrocede, dejando un desierto muerto en el cual solo quedan el cinismo y el rechazo.
>
> Todo lo que necesitas hacer es asegurarte de que tienes las palabras adecuadas para hablar, vestir
>
> la vestimenta adecuada, antes de que finalmente te arrastre.[353]

Los sentimientos de rechazo no son grilletes simplemente figurados. Incluso cuando los ciudadanos son conscientes de las fuerzas que esquilan a la mayoría, el cinismo puede desactivar el cambio político. Cuando esta postura se vuelve lo suficientemente predominante se acomoda en los tendones de la sociedad, afianzando aún más la atomización, impidiendo la solidaridad social y limitando considerablemente las posibilidades políticas.[354] Si se añade la ansiedad a la mezcla, el cóctel resultante se convierte en el más letal de los venenos. El colectivo radical Plan C instalado en el Reino Unido ha redactado un agudo opúsculo titulado "Todos estamos muy ansiosos". El texto une los puntos entre las nefastas condiciones económicas, el trabajo precario, las medidas preventivas contra

los activistas, un énfasis cultural en la autopromoción y un estado de vigilancia abrumadoramente técnico: «Una parte importante de la base social de la ansiedad es la omnipresente red de vigilancia multifacética... Pero esta obvia red es solo el caparazón externo –escriben–. La autoexposición ostensible y voluntaria, a través de las redes sociales, el consumo visible y la elección de posturas en el terreno de las opiniones, asumen asimismo una función en el terreno de la mirada permanente de los otros virtuales.»[355] Cuando este impulso hacia lo panóptico está lleno de una letanía de cuestiones más amplias —desde la creciente desigualdad de la riqueza, las oleadas de recesión e inquietud nacionales y mundiales, y la sombría perspectiva de un desastre medioambiental inducido por el clima— no resulta difícil entender cómo una incertidumbre paralizante, generalizada y alarmante ha llegado a colonizar nuestros estados de ánimo.

Es posible que el cinismo y la ansiedad sean factores extendidos, pero no son omnipotentes ni tampoco omnipresentes; deben enfrentarse cada día a la fricción y la resistencia. Un número incalculable de activistas, inmigrantes, personas desplazadas, refugiados, muchos y diversos desconocidos, artistas y, notablemente, incluso algunos políticos, luchan contra la opresión y presionan contra la embestida emocional que puede conducir con tanta facilidad a esas trampas existenciales. Si no tenemos cuidado, podríamos pintar un cuadro demasiado sombrío y cosificar el cinismo y la ansiedad que estamos intentando desmontar. Bloch insistía en que debemos contribuir a un archivo viviente de esperanza, que nos preocupemos por escuchar y apoderarnos de «algo diferente de la putrefacta y sofocante, cavernosa y nihilista sentencia de muerte».[356]

Cuando tenemos en cuenta que los miembros de Anonymous conocen perfectamente esas condiciones, resulta menos o más destacable que fuesen capaces de sumarse a este “archivo viviente de esperanza”. No estoy en condiciones de decidir si Anonymous atrae a aquellos que tienen vidas emocionales oscuras, o si el entorno de pseudónimos crea un espacio seguro para compartir lo que son simplemente facetas universales de la condición humana. Es probable que se trate de una combinación de ambas. Sin embargo, una y otra vez me sentía impresionada por este emparejamiento de dolor personal con el deseo ardiente de su superación.

Al sacrificar el yo público, rechazar a los líderes y, sobre todo, al negarse a participar en el juego de la autopromoción, Anonymous asegura

el misterio; esto representa en sí mismo un acto político radical, si tenemos en cuenta un orden social que se basa en la vigilancia omnipresente y la celebración del individualismo y el egoísmo incontrolados. La iconografía de Anonymous —mascaras y trajes acéfalos— exhibe visualmente la importancia de la opacidad. *El colectivo* quizás no sea la colmena que a menudo pretende ser y se pretende que sea —y puede estar marcada por las disputas internas— pero aun así Anonymous consigue dejarnos con una sorprendente visión de solidaridad —*e pluribus unum*.*

«Un fuego pequeño necesita una atención constante. Una hoguera puede arder sola. Una conflagración se propaga», manifestó papersplx, un activista de Anonymous. Al adoptar el uso de la máscara, que el sociólogo Richard Sennett observa acertadamente es «uno de los accesorios escénicos más antiguos de la cultura que conecta el escenario y la calle», Anonymous incorporó la dinámica del engaño teatral y la trasladó desde Internet a la vida cotidiana de resistencia.[357] Anonymous se convirtió en un símbolo generalizado para la disensión, un medio para canalizar el profundo desencanto con un dictador, una ley, la economía, la cultura de la violación, básicamente con cualquier cosa. A Anonymous, siempre corriendo riesgos, le gustaba jugar con fuego y muchos de sus participantes despreciaban o rechazaban las medidas de seguridad. No debe sorprendernos que el propio grupo, en su conjunto, finalmente se prendiese fuego, haciendo que el camino para otros ardiese en llamas. Algunos de ellos se quemaron, tanto los participantes como los objetivos. O como lo explica Firefly en el documental *Somos legión*: «Es como el ave Fénix. En ocasiones podía prenderse fuego y quedar reducida a cenizas, pero renacería de esas cenizas. Renacerá aún más fuerte.» Presionar con fuerza contra las reglas y los límites puede llevar a menudo a caer en una trampa o a la desaparición, pero la idea fundamental detrás de la entidad –Anonymous es libre de que cualquiera lo personifique– lo coloca en una excelente posición para la resurrección y la reinvención.

Anonymous ha aparecido muchas veces como una visión, confundiéndonos mientras contemplamos los destellos brillantes de sus encantadores (y ofensivos y confusos) sueños. Es esta facultad de combinar, de una parte, el espacio mítico y, de la otra, la realidad de activistas que asumen riesgos y pasan a la acción, lo que hace que el grupo sea tan atractivo. Desde la distancia es como observar la aurora boreal, una

silenciosa pero mítica batalla de dioses y embaucadores que se libra en el cielo nocturno, un cielo aún más fascinante porque todo el mundo lo puede contemplar. El poder del anonimato epónimo de Anonymous reside en que todos somos libres de elegir si llevamos o no la máscara.

EPÍLOGO

EL ESTADO DE ANONYMOUS

«Con el tiempo he llegado a amar el secreto. Parece ser lo único capaz de hacer misteriosa o maravillosa la vida moderna. Basta ocultar la cosa más corriente para que nos resulte encantadora.»

Oscar Wilde, *El retrato de Dorian Gray*

«La educación política de los técnicos apolíticos es extraordinaria.»

Julian Assange

A muchas personas puede parecerles que el período descrito en este libro representa la máxima expresión de la actividad desarrollada por Anonymous: su función de apoyo a los diferentes movimientos que integraron la Primavera árabe; la enorme atención de los medios de comunicación suscitada por los hackeos desafiantes que protagonizaron los grupos de LulzSec y AntiSec; el compromiso cada vez mayor con las cuestiones relativas a la justicia social nacional comprobados en su implicación contra la cultura de la violación y la brutalidad policial.

Como cabía prever, esta impresionante oleada de actividades de protesta se vio enfrentada a campañas igualmente impresionantes llevadas a cabo por las fuerzas del orden. A través de Europa, Asia, Australia y las Américas, los agentes de la ley detuvieron a más de un centenar de

activistas de Anonymous, incluidas muchas de las figuras retratadas en este libro: Jeremy Hammond y John Borell en Estados Unidos y Ryan Ackroyd y Mustafa Al-Bassam en el Reino Unido. Otras personas detenidas eran activistas extravagantes cuyo "delito" había sido simplemente canalizar una pequeña parte de sus recursos informáticos hacia campañas de DDoS organizadas por Anonymous en un esfuerzo por avergonzar públicamente a algunas entidades financieras, como el caso de PayPal, cuando cedieron a la presión ejercida por el gobierno y suspendieron todos los servicios a WikiLeaks, la sitiada organización de denuncias.

Si lo comparamos con cualquier otro país en el mundo occidental, Estados Unidos actuó con especial agresividad en su persecución legal de los activistas y hackers de Anonymous: las condenas a prisión no solo eran mucho más largas que en otros países sino que iban acompañadas de multas astronómicas. Los activistas estadounidenses de Anonymous como Jeremy Hammond, e incluso los estrategas afiliados al colectivo como el caso de Barrett Brown, se enfrentaron a severas sentencias como consecuencia del hackeo perpetrado contra Stratfor (aunque en su caso momentáneamente). Una vez recuperen la libertad, estas personas continuarán pagando por sus acciones mientras luchan con las pesadas deudas económicas impuestas por sus sentencias.

Estos castigos, combinados con el conocimiento de que el FBI había conseguido utilizar a Sabu, una figura fundamental de Anonymous, como sus ojos y oídos durante meses, provocaron desconfianza, sospechas y temor a que la situación se intensificara en el seno de Anons. Labios sellados. Los grupos de hackers, que siempre habían asumido que había soplones acechando por todos los rincones, se volvieron incluso más paranoicos y reaccionaron reduciendo pertenencia al grupo y aumentando la seguridad en las operaciones que llevaban a cabo. Fundamentalmente, estos grupos también rebajaron el tono de su arrogancia.

En 2013 Anonymous parecía haberse alejado en gran medida de las actividades relacionadas con la infiltración informática. Pero, no obstante, mientras estas acciones se reducían en frecuencia e intensidad, el colectivo continuó actuando, si bien de un modo más moderado. Los Anons italianos continuaron desarrollando sus actividades de hackeo y doseo, y una de las organizaciones más prolíficas de Anonymous orientadas al hackeo, Operation Green Rights, hackeó y desfiguró a docenas de empresas

negligentes con el medioambiente como Monsanto (por razones que no están totalmente claras para mí, estas acciones nunca despertaron demasiada atención en los medios de comunicación ni el consiguiente análisis). No hay duda de que, en 2014 y hasta bien entrado 2015, las actividades más visibles llevadas a cabo por Anonymous en América del Norte y Europa occidental se orientaron hacia la publicidad más que a la acción directa, con un firme énfasis en las operaciones destinadas a concienciar a la opinión pública. En el Reino Unido, la Operación Death Eaters ha procurado llamar la atención sobre el problema del tráfico sexual de niños y el encubrimiento de las actividades de pedofilia llevadas a cabo por algunas de las figuras más poderosas del país. En Estados Unidos, OpFerguson comenzó por apoyar y publicitar las actividades de protesta después de que un oficial de policía disparase y matara a un adolescente afroamericano desarmado llamado Michael Brown. OpISIS, que en muchos sentidos se alinea con los intereses de los poderes estatales occidentales, actúa con el fin de identificar y publicar las cuentas de Twitter y los sitios web de ISIS para eliminarlos de la red.

La clase de hackeos espectaculares que habían sido el billete de entrada directo de Anonymous a la conciencia pública general continuó mereciendo titulares, pero la mayoría de ellos estaban instigados por otros grupos de hackers no afiliados al colectivo. La mayoría de estas entidades tenía muy poco en común con los hackers de Anonymous, cuyos objetivos habían sido la justicia social o una acción directa políticamente destacada. De hecho, muchos de ellos eran directamente antagónicos a esas agendas. En 2014, Sony Pictures Entertainment se convirtió en el objetivo de los hackers cuando los misteriosos Guardianes de la Paz hicieron aflorar una enorme cantidad de información sensible de la empresa, supuestamente como represalia por el planeado estreno de una película que satirizaba al gobierno de Corea del Norte. Los hackers revelaron el contenido de la caché a la opinión pública: desde copias de preselección de próximas películas hasta reuniones informativas internas y correos electrónicos de la empresa. Durante la temporada de vacaciones de 2014, Sony volvió a ser objetivo de varios ataques cuando Lizard Squad —un grupo evocador de LulzSec pero que carecía de una agenda política manifiesta— entretuvo a sus seguidores en Twitter desactivando la PlayStation Network con un ataque masivo de DDoS el día de Navidad. En enero de 2015, un grupo de

hackers pro ISIS conocido como CyberCaliphate, secuestró una cuenta de Twitter del gobierno de Estados Unidos, en febrero una cuenta de *Newsweek* y en abril hasta consiguieron hacerse con el control total de una cadena de televisión francesa.

Pero las apariencias pueden ser engañosas. Los hackeos en nombre de Anonymous no han cesado; eran simplemente menos visibles. En Latinoamérica y partes de Asia, los hackers de Anonymous, la mayoría de los cuales llevaba algún tiempo activa, continuaron abriéndose camino dentro de los sistemas informáticos. Uno de los equipos más prolíficos, LulzSec Perú, llevó a cabo docenas de operaciones, incluido el requisamiento de la cuenta de Twitter del presidente de Venezuela, Nicolás Maduro, y el hackeo de documentos pertenecientes a la Fuerza Aérea de Chile. Su hackeo más memorable se materializó el 11 de febrero de 2014, cuando revelaron públicamente correos electrónicos que demostraban la corrupción en el seno del gobierno peruano. Según informó Frank Bajak de la agencia Associated Press, los correos electrónicos filtrados de la red del Consejo de Ministros peruano provocó un «escándalo nacional» y «alimentó las acusaciones de que importantes ministros del Gabinete nacional habían actuado más como lobistas industriales que como funcionarios públicos. Esta situación ayudó a precipitar un voto de censura... al que el Gabinete nacional sobrevivió a duras penas».[358]

Si bien este hackeo era un motivo más que suficiente para atraer la atención de los periodistas de habla inglesa, la gran mayoría de los medios de comunicación occidentales ha permanecido ajena a las actividades que Anonymous ha desarrollado en el extranjero. Por supuesto, incluso los periodistas que quieren cubrir estos hechos no cuentan habitualmente con capacitación suficiente para llevar a a cabo su trabajo. Las barreras idiomáticas combinadas con la dificultad para acceder a los hackers —más reticentes que nunca después de la oleada de arrestos— provocaron que el tipo de información que era común durante el período de actuación de LulzSec resultara mucho más complicada de reproducir.

La falta de interés por parte de los medios de comunicación podría significar menos un signo de que Anonymous ha ralentizado sus actividades, y más un signo de que simplemente ha mejorado sus habilidades para la supervivencia. Aunque gracias a sus propias iniciativas publicitarias sabemos que AntiSec y LulzSec eran fuerzas a las que había

que tener en cuenta, su carácter excesivamente público era, en última instancia, su mayor debilidad. Puede resultar complicado sopesar las ventajas e inconvenientes inherentes a cada enfoque. Al captar la atención, LulzSec y AntiSec pudieron exponer sus causas y también inspirar a otros para que se uniera a ellos o siguieran su ejemplo. Pero cuanto más tiempo trabajaban estos equipos estables bajo el intenso y vigilante control de los medios de comunicación, del público y, especialmente, del eEtado, más susceptibles se volvían a su captura. Con cada hackeo público y con cada burla —especialmente cuando muchas de ellas estaban dirigidas a las fuerzas del orden— la presión para identificarles y detenerles fue in crescendo.

Pero, tal como ocurre con cualquier movimiento político incipiente cuyos estilos y enfoques organizativos no han sido puestos a prueba, los escarceos de Anonymous con la fama y otras tácticas agresivas eran necesariamente experimentales. No es de extrañar que los resultados oscilaran entre el éxito espectacular y el fracaso más estrepitoso. Con los inevitables traspiés se produce el daño colateral, pero los activistas pueden aprender de sus propios errores y también de los errores cometidos por los demás.

Y parece que al menos algunos han estado prestando atención a lo que pasaba. Tomemos, por ejemplo, el hackeo de 2014 contra el Gamma Group, una empresa británica de spyware o programas espía dedicada a la venta de “soluciones de vanguardia en materia de control [y] vigilancia técnica”[359] a los gobiernos, incluidos regímenes dictatoriales y represivos que se sabe que utilizan esas herramientas contra activistas y disidentes. En 2011 esta empresa de software adquirió notoriedad cuando WikiLeaks publicó uno de los vídeos promocionales de la compañía junto con folletos y presentaciones que demuestran cómo puede utilizarse su software para infectar un ordenador.[360] Poco después, dos investigadores en temas de seguridad sugirieron que era posible que el gobierno de Bahrein hubiese empleado este método para entregar subrepticiamente un programa llamado FinFisher a los activistas locales a través de archivos adjuntos de correos electrónicos. (En respuesta a esta cuestión, Gamma afirmó que el programa podía haber sido robado ya que los representantes de la empresa insistieron en que ellos nunca le vendieron el FinFisher a Bahrein.)[361]

El 3 de agosto de 2014, un hacker que se hacía llamar Phineas Fisher

(Phineas es el nombre de un vidente de la mitología griega) apareció de pronto en la red y anunció en numerosas plataformas de las redes sociales que había conseguido entrar en los sistemas informáticos de Gamma y estaba revelando cuarenta gigabytes de datos relacionados con FinFisher. La extensa colección de documentos incluía material técnico (especificaciones de software, códigos fuente, documentación, análisis de uso) junto con listas de clientes, listas de precios, tutoriales y mucho más. Entre otras revelaciones, el hackeo de Phineas Fisher ayudó a reforzar la evidencia de que el gobierno de Bahrein había utilizado el programa FinFisher contra los activistas.[362]

En una declaración publicada junto con la filtración, Phineas Fisher exhortaba a sus colegas hackers a "devolver el hackeo" y les daba algunos consejos. ¡Devolver el hackeo!: una guía "Hágalo-Usted-Mismo *(DIY) para aquellos que no tienen paciencia para esperar a los denunciantes* comenzaba con el siguiente consejo:

> Seguid siempre el sentido común, nunca hagáis ningún hackeo relacionado fuera de Whonix, nunca hagáis nada de vuestro uso informático normal dentro de Whonix, nunca mencionéis ninguna información sobre vuestra vida real cuando habléis con otros hackers, y nunca os jactéis de vuestras proezas de hackeo con los amigos en la vida real: entonces podréis hacer prácticamente lo que queráis sin temor a ser v& [*vanned*: un térimo que se refiere a ser allanado o detenido por las fuerzas de la ley].[363]

Aunque Phineas Fisher no estaba alineado de manera explícita con Anonymous, su hackeo representaba el espíritu del grupo y era sin duda deudor del particular estilo de filtración que habían inaugurado LulzSec y otros grupos de Anonymous. (Phineas Fisher también ha dado muestras de ser un experto en el lulz cuando escribió su breve manifiesto: «Fue solo después de haber errado en hackear completamente Gamma y acabar en posesión de algunos documentos interesantes pero ninguna copia del software del servidor de FinSpy que tuve que arreglármelas con el plan B mucho menos lulzy de filtrar su material mientras me burlaba de ellos en Twitter».)[364] En el contexto de un notable resurgimiento en los últimos años de las actividades relacionadas con filtraciones y denuncias,

fundamentalmente a cargo de ciudadanos tan valientes como Chelsea Manning y Edward Snowden, la modalidad de filtración practicada por Anonymous era característica por su arriesgado componente de acción directa: en lugar de filtrar archivos confiados a ellos, se infiltraban en las redes de corporaciones y gobiernos con el propósito de extraer información de las empresas de seguridad e inteligencia.

Donde Phineas Fisher se diferenciaba de grupos como LulzSec y AntiSec no era en el método o la elección del objetivo, sino más bien al demostrar mucho más cuidado, precisión y cautela de lo que Anonymous jamás había hecho. Además, en lugar de emplear su tiempo bajo los focos para autopromocionarse, Phineas Fisher volcó los datos en Twitter y reddit, trabajó durante cinco días para llamar la atención sobre el material filtrado y luego simplemente se esfumó.

Es decir, hasta que volvió a aparecer el 5 de julio de 2015 para reclamar la autoría de un hackeo similar, en esta ocasión con la vista puesta en otro proveedor de armas para la guerra cibernética, incluso más vilipendiado, llamado Hacking Team. La empresa de software y seguridad instalada en Milán vende lo que describe como "soluciones ofensivas" a una serie de clientes, desde el FBI hasta el ejército de Estados Unidos.[365] En esta ocasión, Phineas Fisher consiguió acceder a su cuenta de Twitter, cambió el nombre de la empresa de Hacking Team (equipo hackeador) a Hacked Team (equipo hackeado) y adoptó su identidad para hacer un anuncio: «Puesto que no tenemos nada que ocultar, estamos publicando todos nuestros correos electrónicos, archivos y códigos fuente [enlace].»[366] Con anterioridad a que se produjera el hackeo, estos tecnólogos mercenarios habían hecho todo lo posible para ocultar la naturaleza especial de sus servicios, tratos y clientes. Gracias a los masivos 400 gigabytes de datos liberados, todo eso ha cambiado. Al igual que sucedió en el caso de GammaGroup, Hacking Team declaró públicamente que la empresa nunca vende productos a los regímenes represivos. Ahora sabemos que no es así. De acuerdo con los datos filtrados, la empresa efectivamente les vendía productos a esos gobiernos sin ningún escrúpulo y participaba de muchas otras prácticas cuestionables, incluidas el acaparamiento de vulnerabilidades informáticas críticas —incluidas dos en el omnipresente reproductor Adobe Flash— que podían utilizarse contra millones de usuarios de Internet.

Para demostrar que era Phineas Fisher (y sugerir al mismo tiempo que aún habría más) tuiteó desde la cuenta que había creado previamente para burlarse de Gamma Group ("GammaGroupPR"):«gamma y HT caídos, aún quedan algunos más :)».[367] Fisher también se reconectó a su manifiesto/manual HUM ¡*Devolver el hackeo*. Las máximas contenidas en el manual de Phineas Fisher no son nuevas. Se conocen desde hace tiempo y han sido adoptadas en los círculos hacker, incluida la élite de hackers de Anonymous (varios de los cuales, hay que decirlo, nunca han sido atrapados y siguen en libertad). No obstante, teniendo en cuenta la dificultad que comportan la aplicación de medidas de seguridad y los arrestos de hackers de Anonymous, uno podría reconocer una cierta prudencia a la hora de repetir una y otra vez estos principios básicos. Y de manera muy similar a la que Phineas Fisher ha suplicado a sus colegas hackers que pongan en práctica medidas de seguridad excepcionales, Anonymous, después del Sabutaje de 2012, ahora advierte continuamente a sus neófitos que se tomen en serio la cuestión de la seguridad. «Si eres sangre nueva –tuiteó Anon2earth entonces– tranquilo, relájate y observa. No participes de ninguna operación a menos que sepas qué coño estás haciendo. Protégete.»[368] En los círculos de Anonymous, los consejos y amonestaciones relacionados con la seguridad forman parte hoy del contexto rutinario de las conversaciones cotidianas.

Lejos de tratarse de eslóganes vacíos de contenido, al parecer estas lecciones han sido acatadas no solo por hackers como Phineas Fisher, sino también dentro de las filas de Anonymous. Tomemos por ejemplo el caso de OpCyberPrivacym, una campaña general contraria a las leyes de vigilancia occidentales como el proyecto de ley C-51 de Canadá, propuesto en 2015 y criticado por académicos, abogados, periodistas y docenas de grupos de la sociedad civil por otorgarle un poder excesivo a las fuerzas del orden y las agencias de inteligencia. Al principio, Anons trató de atacar este proyecto de ley solo a través de la publicidad, pero al no conseguir avanzar por ese camino ni obtener la atención de los medios de comunicación, el colectivo decidió resucitar una táctica clásica de Anonymous: el DDoS.

El 17 de junio de 2015, Anonymous desactivó docenas de sitios web del gobierno canadiense, incluidos los del Servicio de Inteligencia y Seguridad del Canadá (CSIS) y de los departamentos de Justicia, Industria, Comercio y Desarrollo, Recursos Naturales y Asuntos Exteriores. Y lo que

es más importante, Anonymous consiguió interrumpir las comunicaciones digitales mediante un ataque deliberado a un servidor de correo electrónico. La campaña se aseguró una extensa cobertura. Según *The Globe and Mail*, «se trató del ciberataque más importante realizado en este país desde que el año pasado hackers chinos apoyados por el Estado irrumpieron en la principal agencia de investigación científica del Canadá».[369] Poco después de la campaña, uno de sus organizadores me explicó que «el grupo de trabajo principal» había estado colaborando estrechamente «durante cerca de siete meses» en varias operaciones: «desde cazar a polis de Ferguson, la revolución en Ucrania, las mierdas del Ku Klux Klan y la caza de pedófilos, hasta cuestiones relacionadas con la privacidad». Algunos de los Anons eran novatos, mientras que muchos de los que formaban el grupo principal habían estado actuando durante muchos años en el colectivo. En abierto contraste con lo sucedido en diciembre de 2010 durante la Operación Venganza contra PayPal, que acabó con el arresto de multitud de participantes, insistió en que la seguridad era una prioridad tan urgente que uno de sus objetivos era evitar todos los daños colaterales, cualquier cosa que los agentes de la ley pudieran utilizar para acentuar su respuesta. Concluyó la conversación por chat observando con orgullo que no se había producido «ningún fallo [de seguridad] hasta ahora. Lo cual está muy bien». Más tarde me confesó que ya habíamos chateado en el pasado, pero que él había utilizado un apodo diferente entonces y me explicó que, a partir de ahora, nuestros nombres serían tratados como teléfonos móviles quemados: desechados periódicamente de modo que, cuando aparece un activista nuevo será, en esencia, un Anon diferente y al que resulte más difícil relacionar con cualquier operación anterior.

Sin los arrestos producidos en 2011 y 2012 resulta difícil imaginar que se hubiesen implementado unas medidas de seguridad tan meticulosas y aún queda por ver también cuán eficaces pueden ser. Al parecer, muchos en Anonymous todavía no están seguros de qué es lo que pueden conseguir y qué es exactamente lo que está en juego. Gran parte de esta evaluación dependerá del tratamiento que reciban aquellos que ya han sido arrestados y de cuál sea su destino en términos jurídicos.

En el caso de PayPal 14, la mayoría de acusados se libró por poco de cumplir condena en prisión. Once de los trece acusados se declararon culpables de un delito y un delito menor (los cargos por delitos mayores

fueron retirados posteriormente ya que cumplían las estipulaciones establecidas en el trato negociado). Otros dos acusados fueron condenados respectivamente a tres y cuatro meses en centros correccionales, lo que les permitió evitar una condena por delito mayor. Los trece tuvieron que pagar 5.600 dólares en concepto de restitución a eBay (ex sociedad matriz de PayPal), y a aquellos que no pudieron hacer frente a esta multa en un único pago se les exigió un pago mensual de cien dólares. El decimocuarto miembro del grupo, Dennis Owen Collins, era uno de los miembros más dedicados de AnonOps (en este libro aparece como “Fred” y “Owen”). Collins falleció el 16 de julio de 2015, mientras cumplía un año de arresto domiciliario, a la edad de 54 años, después de haber librado una dura batalla con una enfermedad pulmonar crónica y debilitante que le aquejó durante buena parte de su vida adulta.

De todos los casos registrados en Estados Unidos relacionados con Anonymous, hay uno que sobresale por encima de todos: el de Barrett Brown. El 22 de enero de 2015, en una sala de los juzgados de Dallas llena hasta la bandera, El juez Samuel Lindsay pronunció una dura sentencia contra el demagógico periodista y activista. Brown, que en el momento de emitirse la sentencia ya había pasado más de dos años entre rejas, recibió un pena adicional de treinta y cinco meses de cárcel y una multa de casi un millón de dólares en concepto de indemnización a pagar a Stratfor, la empresa de inteligencia víctima del hackeo. Brown, que originalmente se enfrentaba a diecisiete cargos, después de haber aceptado un acuerdo de culpabilidad que reducía a ocho años de prisión la posible condena, al final fue condenado solamente por tres delitos: proferir amenazas contra un agente del FBI, obstrucción a una orden de registro y colaboración con los hackers de Anonymous que se infiltraron en la empresa de inteligencia de Austin, Texas, y robaron información de su sistema informático.

El dato más excepcional —y más cuestionable— de todo este asunto fue la acusación formulada por el juez de que Brown «había hecho algo más que simplemente informar acerca de las actividades de los hackers», había ayudado a organizarles: «El tribunal concluye que el Sr. Brown colaboró con los hackers y los apoyó para identificar los objetivos, prestó asesoramiento, formuló una estrategia y ayudó a organizar sus actividades.»[370]

Sin embargo sigue vigente el hecho de que Brown no era un hacker, y

tampoco fue acusado oficialmente de ningún delito relacionado con actividades de hackeo. El papel de Brown en Anonymous era el de un apasionado estratega. No había ni una sola evidencia sólida de que hubiese coordinado —mucho menos participado— en la infiltración efectiva de Stratfor, que se llevó a cabo en diciembre de 2011. Brown estaba interesado principalmente en los correos electrónicos, si bien publicó un enlace a números de tarjetas de crédito robadas por los hackers de Anonymous y en un momento dado se enfrentó a un cargo criminal por ese hecho. De los diecisiete cargos a los que se enfrentaba inicialmente, éste era el más polémico: él no había robado ni utilizado la información de esas tarjetas de crédito, sino que simplemente trasladó de una sala de chat a otra un enlace ampliamente difundido. A pesar de que ese cargo fue desestimado en marzo de 2014, el juez coincidió no obstante con los argumentos de la acusación en el sentido de que ese enlace con los datos robados había ayudado a los hackers y que, por lo tanto, debía ser considerado como un elemento relevante para la sentencia general. Se trató de «algo más que aquel simple posteo» razonó el juez. «Se trata de su implicación con los otros actores que estaban involucrados en esa misma actividad.»[371] En consecuencia, incluso sin este cargo en su contra, la severidad de la sentencia de Brown fue mayor.

Esta contorsión y oscuridad jurídicas afectan claramente la libertad de expresión y crea una situación en la que otros periodistas se mostrarían menos proclives a compartir enlaces por temor a que esa actividad pudiera ser considerada por un tribunal como agravante de un delito. (Una vez conocido el fallo, la periodista Quinn Norton anunció que dejaría de informar acerca de fallos de seguridad, seguridad informática o hackers por temor a sufrir una represalia similar por parte del gobierno.)[372] Al igual que tantos otros hackers, denunciantes, periodistas y hacktivistas que lo arriesgaron todo por defender la libertad de prensa y la rendición de cuentas, Brown está pagando actualmente un precio excesivo; la sentencia habla de la voluntad del Estado de procesar no solamente a los hackers que tienen una motivación política, sino también a los geeks y periodistas como Brown que trabajan estrechamente con ellos.

El duro tratamiento jurídico aplicado a hackers activistas y simpatizantes estadounidenses como Hammond, Brown y otros se encuentra en el centro de un caso en marcha mientras escribo este epílogo.

El 15 de julio de 2015, un hacker británico llamado Lauri Love fue arrestado en su país y ahora se enfrenta a la extradición a Estados Unidos, donde ha sido acusado en el marco de la Ley de Fraude y Abuso Informático en Nueva Jersey por haber hackeado presuntamente a la NASA, al ejército de Estados Unidos y a la Reserva Federal como parte de la OpLastResor de Anonymous, impulsada a raíz del suicidio del hacker Aaron Swartz. Los partidarios de Love están haciendo todo lo que está en su poder para frenar su extradición, preocupados por el hecho de que si es extraditado a Estados Unidos —donde las penas son mucho más severas— podría tomar también el trágico camino elegido por Swartz. «Extraditar a Lauri Love a Estados Unidos –insisten– sería una grave violación de sus derechos, tanto humanos como civiles.»[373]

El Estado ha dependido desde hace mucho tiempo de la extralimitación procesal y la represión con el fin de crear un clima de miedo capaz de aplastar a los movimientos políticos o, al menos, de limitar su crecimiento. Por lo tanto, resulta tal vez destacable que un número tan importante de geeks y hackers no solo no se haya sentido intimidado por la respuesta de las fuerzas de la ley sino que, por el contrario, esa respuesta les haya impulsado a la acción. Las revelaciones aportadas por Snowden, en particular, han sido vividas por geeks y hackers como una llamada de alerta histórica y apremiante: les ha proporcionado un enfoque y una vitalidad renovados, revitalizando la búsqueda de agendas que protegen la privacidad a través del desarrollo de herramientas de encriptación.

Desde que se produjeron los arrestos, muchos ex miembros de Anonymous, LulzSec y AntiSec han seguido contribuyendo afanosamente a este movimiento que defiende la privacidad. Durante el verano de 2015, Donncha O’Cearbhaill fue escogido por Tor, el principal proyecto de encriptación, para que trabajase como pasante de verano bajo la dirección de uno de los desarrolladores veteranos del proyecto. En el curso de una entrevista con la organización, a Donncha le preguntaron, «¿Quiénes son tus héroes —si es que tienes alguno— en el software libre de Internet?» O’Cearbhaill respondió honrando a aquellos con los que trabajaba directamente y a la comunidad de hackers en su conjunto: «Me inspira el trabajo de mucha gente en la comunidad que defiente la libertad en Internet. Me siento especialmente agradecido a personas como Edward Snowden, Julian Assange y Jeremy Hammond, quienes han realizado enormes

sacrificios para tratar de arrojar luz sobre el creciente estado de vigilancia. Me siento inspirado por los desarrolladores y defensores de software libre en cualquier parte del mundo, quienes continúan intentando hacer algo sobre esta cuestión.»[374] Mustafa Al-Bassam, que sigue trabajando como becario en Privacy International, ha diversificado sus contribuciones. Después de que se filtrasen a la opinión pública los archivos de Hacking Team, los alojó en un sitio, asegurándose de que continuasen disponibles para su descarga. Los archivos tuvieron una gran demanda; su sitio fue atacado durante días, obligándole a trabajar sin descanso para mantenerlo. Al-Bassam también colabora con investigadores de seguridad y otros ex Anons, incluido Darren Martyn, a través de un *think tank* informal de hackers llamado LizardHQ. Hasta ahora han llamado la atención sobre herramientas de vigilancia cuestionables y sus vulnerabilidades, incluido Hola (un VPN con diez millones de usuarios que también resulta que contiene una puerta trasera con la que reclutar ordenadores de usuarios para incorporarlos a botnets); E-Detective (un producto de interceptación legal que utilizan los militares chinos y más de un centenar de fuerzas policiales internacionales); e Impero (un software espía utilizado por una parte de las escuelas británicas para espiar a los estudiantes). Al-Bassam me explicó que el propósito de las actividades que lleva a cabo LizardHQ es «exponer las vulnerabilidades que permiten que esto suceda para que la gente pueda tomar decisiones informadas sobre los sistemas en los que participa y que ignoran sus libertades civiles... Nosotros no coordinamos la divulgación de las vulnerabilidades con los proveedores que desarrollan software espía, ni tampoco les informamos previamente, porque eso establecería un mal precedente de investigadores de seguridad que cooperan con proveedores de software espía.»

Como lo confirman numerosos estudios y encuestas realizados sobre esta cuestión, desde que se produjeron las revelaciones de Snowden la mayor parte de la opinión pública estadounidense está más preocupada que antes por la preservación de la privacidad.[375] Y las Naciones Unidas también ha intervenido en esta cuestión; su Oficina del Alto Comisionado publicó un informe en el que defiende la santidad democrática de la encriptación, por su capacidad para «proporcionar la privacidad y seguridad necesarias para el ejercicio del derecho a la libertad de expresión y opinión en la era digital».

Y sin embargo, mientras el tribunal de la opinión pública cambia, las fuerzas de la ley y otros funcionarios del gobierno están respondiendo como era previsible —y del mismo modo que lo han hecho durante décadas— demonizando tanto a las tecnologías relacionadas con la encriptación como a los ideales de anonimato asociadas a ellas. En respuesta a la presión ejercida por los usuarios, las empresas propietarias de software como Apple y Google han realizado grandes esfuerzos para promover la seguridad del usuario, provocando de esta manera la insistente respuesta hostil por parte del FBI y otras agencias defensoras de la ley, en el sentido de que las corporaciones, en cambio, tienen la obligación de «impedir la encriptación por encima de todo». En octubre de 2014, el director del FBI pronunció un discurso alarmista y mordaz sobre el tema de la privacidad en la Brookings Institution en Washington, DC: «Con Going Dark*, aquellos de nosotros que trabajamos en el cumplimiento de la ley y la seguridad pública tenemos la enorme preocupación de estar perdiendo… estar perdiendo a los depredadores que explotan a los más vulnerables de entre nosotros... perdiendo a los criminales violentos que atacan nuestras comunidades... perdiendo a la célula terrorista que utiliza las redes sociales para reclutar, planificar y ejecutar un ataque.»[376]

Dicho de otro modo, actualmente se está librando una verdadera batalla campal en el terreno de las libertades civiles respecto del futuro de la privacidad y el anonimato. Esta lucha, por supuesto, no es nueva. Pero hace solo muy poco que ha escapado de los enrarecidos hábitats de teóricos jurídicos, responsables políticos, tecnólogos y académicos para incorporarse a un ámbito más general de colectivos tecnológicos, abogados, periodistas, cineastas, hackers, desarrolladores de software y hardware, ONG y ciudadanos privados sensibilizados. De una manera similar a como los ideales de la libertad de expresión penetraron en la conciencia pública durante las batallas campales políticas —como las que libraron en Spokane los Trabajadores Industriales del Mundo a comienzos de la década de 1900, o como las protestas en favor de la libertad de expresión que tuvieron lugar en los años sesenta en la Universidad de Berkeley— las iniciativas de base relativas a la privacidad parecen estar alcanzando la masa crítica.

La postura de Anonymous dentro de este recién acuñado movimiento colectivo defensor de la privacidad merece un examen más detenido. Por supuesto, teniendo en cuenta su homónimo y simbolismo, la propia

existencia de Anonymous confirma un compromiso con los valores asediados. Pero tener a una entidad como Anonymous tan estrechamente vinculada a un movimiento social representa, en muchos sentidos, una espada de doble filo: si bien Anonymous puede popularizar diversas cuestiones y atraer miembros al colectivo, pueden asimismo despertar las críticas de sus detractores. Teniendo en cuenta su tendencia a provocar la contención, es algo que cabe esperar. Es imposible ignorar las controversias que provoca Anonymous, e incluso cuando su intención es hacer precisamente eso, los resultados pueden llegar a ser imprevisibles, improductivos y, en algunos casos, hasta perjudiciales.

Sin embargo, más que cualquier otro movimiento político, pasado o presente, Anonymous representa el estudio de caso ideal a través del cual explorar el funcionamiento, los beneficios, las contradicciones y las limitaciones del anonimato en acción aplicado. Y a medida que este movimiento de la privacidad se une, he observado una clara tensión entre aquellos que creen en el anonimato como una herramienta políticamente útil. Aunque muchos defensores izquierdistas y liberales apoyan de manera inequívoca el derecho a la encriptación, en ocasiones también expresan un profundo molestar respecto del uso del secretismo entre activistas, el papel del anonimato en general y la función de Anonymous en particular. Para decirlo de un modo ligeramente distinto, muchos se sienten molestos con la manera en la que Anonymous, y las acciones anónimas en términos generales, no rinden cuentas o, en una versión más categórica de la crítica, demuestran una cobardía esencial. Un académico expresó recientemente sin rodeos su malestar con el anonimato al declarar que «lo opuesto del anonimato es la responsabilidad».

Si bien la asociación entre anonimato e irresponsabilidad es una cuestión mucho más compleja de lo que la declaración implica, resulta innegable que un rasgo esencial del encubrimiento intencional en la red es la capacidad de evadir la atribución de responsabilidades. La académica e investigadora en el tema de la privacidad Helen Nissenbaum ha defendido el anonimato por estos mismos motivos: «El valor del anonimato –afirma Nissenbaum– no reside en la capacidad de ser anónimo sino en la posibilidad de actuar o participar manteniéndose fuera del alcance, permaneciendo inaccesible.»[377]

Aunque algunas formas limitadas de secretismo y protección ante las

repercusiones legales son vitales para Anonymous, los arrestos de los miembros de LulzSec y otros participantes han dejado muy claro a los Anons actuales que el anonimato nunca es absoluto. Muchos Anons son conscientes del riesgo y, por tanto, actúan siempre teniendo en cuenta las consecuencias futuras que pueden acarrear sus acciones: enmarcando su actividad como si estuviesen seguros de que será descubierta, aun cuando esperan que quizás no sea así. Y, en algunos casos, los Anons renuncian incluso al intento de este anonimato estricto, técnico y motivado por razones de seguridad, optando en cambio solo por el anonimato social que les permite interactuar con otros Anons de manera igualitaria. Un miembro del PayPal 14, Keith Wilson Downey, reconoció esta situación complicada al razonar su participación en la Operación Venganza: «Como defensor de la libertad de información durante más de una década, decidí que iba a hacer algo más que simplemente hablar. De modo que, el 9 de diciembre de 2010 descargué LOIC, me conecté a la colmena y me uní a la protesta contra PayPal. Merece la pena señalar asimismo que decidí no cubrir mis huellas, ya que consideré que se trataba de una protesta legítima que merecía el riesgo. Y es una decisión que ha cambiado mi vida durante los tres años siguientes.»[378] Para Downey, el anonimato no era un caparazón para escapar de la responsabilidad sino un marco que posibilitaba la acción.

Es difícil reducir el funcionamiento del anonimato dentro de Anonymous a una lógica simple: cualquiera que sea la formulación que se proponga, siempre puede ser adoptado y reeditado de diferentes maneras y orientado hacia fines diferentes, por cualquiera que desee utilizarlo. Nunca puede ser poseído, mucho menos controlado, porque cualquier intento de hacerlo lo alterará convirtiéndolo en algo diferente al anonimato; de alguna manera el propio ideal es, en consecuencia, incorruptible (o infinitamente corruptible), siempre lejos del alcance del poder, incluso si aquellos que lo experimentan temporalmente, o que creen que lo están experimentando, pueden ser detenidos. No obstante, Anonymous ha generado claramente una nueva postura en materia política, cuyo objetivo es superar el «discurso» como lo expresó Downey, donde las *acciones* importen, y las acciones puedan ser evaluadas, pero las identidades que hay detrás de ellas —incluso cuando sean identificables y expuestas a prisión— sean reconocidas por todos los implicados como menos importantes que las acciones que llevan a cabo. De este modo, incluso cuando los individuos son nombrados, el valor

del anonimato que una vez creyeron disfrutar queda preservado en las acciones que les permitió llevar a cabo. Creer en la idea de Anonymous es suficiente para motivar la acción, incluso si el anonimato total no es el objetivo o es inalcanzable.

Si bien los participantes de Anonymous están cubiertos por un seudónimo siempre que actúan en público, resulta fundamental también destacar que la mayoría de las propias acciones no se lleva a cabo en secreto. Estos activistas se organizan en canales de chat públicos, publican comunicados de prensa, anuncian sus causas y ofrecen sus razones en vídeos impactantes. También están habitualmente en contacto directo con activistas y periodistas locales que no pertenecen a Anonymous. Durante los primeros días de la OpFerguson, por ejemplo, la CNN estaba en contacto con los participantes en el IRC, tratando de seducirles para que aparecieran en directo en televisión. Resulta difícil imaginar que un periodista pudiera ser capaz de asegurar un acceso inicial similar con terroristas o hackers delincuentes de sombrero negro que buscan —a cualquier precio— eludir cualquier contacto con el Estado y el público en general. La mayoría de Anons, en otras palabras, no se está ocultando en el equivalente en Internet de las cuevas de Tora Bora, intrigando en la más absoluta oscuridad. Actúan fundamentalmente a plena luz del día, aunque con ciertas medidas de seguridad, solo las suficientes para permitirles llevar a cabo sus acciones.

Habitualmente también es fácil asociar operaciones concretas con grupos, cuentas de Twitter, redes de IRC o personas específicos. Como ejemplo de esto podemos recurrir nuevamente a la OpCyberPrivacy. Poco después de que el grupo que estaba detrás de esta OP completase una serie de ataques de DDoS en protesta por el proyecto de ley canadiense C-51, otro hacker de Anonymous conocido como ro0ted anunció que había hackeado un sitio web del gobierno de Canadá e hizo públicos los nombres y credenciales de los empleados. Al principio, los periodistas atribuyeron esta operación de hackeo a la OpCyberPrivacy de Anons. Pero sus participantes, que no tenían nada que ver con el hackeo —y, de hecho, criticaron con vehemencia la acción, a la que calificaron de irresponsable por su vulneración de la privacidad— se pusieron de inmediato en contacto con el mencionado periodista para que corrigiese la información. Como habría revelado cualquier investigación superficial, ro0ted afirmó estar

vinculado a Anonymous. Pero no a OpCyberPrivacy, sino más bien a la red de ciberguerrilla de Anonymous.[379] La mayoría de los artículos sobre esta cuestión fueron corregidos rápidamente y una de las características de Anonymous quedó clara para todos aquellos que estuviesen prestando atención: la responsabilidad puede buscarse incluso entre aquellos que conservan una pizca de anonimato.[380]

Aun cuando la mayoría de las acciones ejecutadas bajo el manto de Anonymous pueda relacionarse con alguna entidad receptiva, muchos observadores siguen expresando su preocupación sobre la rendición de cuentas cuando en última instancia no existe ningún recurso a la identidad legal. Una pregunta que me hacen a menudo es la siguiente: si Anonymous es un colectivo clandestino, ¿como puede ser responsable ante las comunidades con las que trabaja?

Sin embargo, merece la pena considerar en qué medida es factible esta responsabilidad en comunidades que exhiben una transparencia y una rendición de cuentas evidentes. Para demostrar aun más este punto, pensemos en el ámbito del periodismo, a menudo presentado como la empresa transparente por excelencia. Los periodistas publican noticias con sus nombres legales y la credibilidad de los medios de comunicación depende de que ellos publiquen hechos, no mentiras. Y aun así se acepta como una necesidad —incluso como un derecho sacrosanto— que los periodistas puedan confiar también de manera selectiva en fuentes anónimas, sobre todo cuando el acceso o la información no se pueden conseguir si no se cuenta con ellas.

Los periodistas, incluso con estas premisas, cometen ocasionalmente actos similares a aquellos de los que también se acusa a Anonymous: divulgar los nombres de individuos sensibles y, de este modo, ponerlos en peligro de ser doxeados. Esta táctica (comprensiblemente) es una de las prácticas más controvertidas de Anonymous y, en ocasiones, una de las más desagradables. Como se ha indagado en este libro, el doxeo afecta a menudo a otros dentro del propio Anonymous, especialmente cuando alguien divulga nombres de espectadores inocentes o atribuye una acción de manera equivocada. Esto fue precisamente lo que ocurrió con la OpFerguson cuando una cuenta de Twitter de Anonymous, TheAnonMessage, divulgó el nombre y fotografías de un agente de policía en la creencia errónea de que era el responsable de haber disparado contra

Michael Brown.

Incluso si a los periodistas jamás se les acusa de doxeo propiamente dicho, a veces el efecto es el mismo y es un error que cometen no solo los periódicos sensacionalistas o los sitios de noticias como Gawker, cuyo fundador se jactó en una ocasión diciendo, «tengo una simple prueba de fuego editorial, que es: ¿es verdad y es interesante?».[381] En 2014, el mismo año en que Anonymous doxeó equivocadamente al oficial de policía de Ferguson, el doxeo más notable del año no fue obra de Anonymous sino de *Newsweek*.

La revista relanzó con gran pompa su edición impresa en marzo de 2014 con una importante noticia de portada: sus periodistas habían descubierto supuestamente la verdadera identidad de Satoshi Nakomoto, el famoso fundador de la criptodivisa Bitcoin, que se ocultaba detrás de un seudónimo. *Newsweek* insistía en que, en realidad, el nombre de usuario no era totalmente un seudónimo: que Dorian Nakamoto, un ingeniero japonés-americano ya mayor que vivía en el sur de California, era el hombre esquivo y la mente que estaban detrás de la popular divisa digital. La investigación, la historia y las consecuencias fueron profundamente intrusivas, adoptaron la lógica de una operación de doxeo instigada por un hacker. La periodista de investigación Leah McGrath Goodman, publicó una fotografía de la casa de Nakamoto, en la que aparecía la dirección de una calle perfectamente legible y la matrícula de un coche. La tarea de localizar a Nakamoto después de hacerse públicos estos datos fue muy sencilla. Y esta información fue ampliada todavía más a través de una maraña de detalles privados relacionados con sus finanzas, estado de salud y problemas matrimoniales, todo ello aireado a millones de estadounidenses. Posteriormente, *Los Angeles Times* participó en una “caza de Bitcoin” junto a otros medios informativos, durante la cual acosaron a Dorian en su casa, le sitiaron con fotógrafos, le siguieron hasta un ascensor para interrogarle y, más tarde, se mofaron de él por escrito por salir de su casa y ofrecerle a uno de los periodistas que le acosaban una entrevista a cambio de un almuerzo gratis.

Gran número de expertos, periodistas y observadores cuestionaron a *Newsweek* por la endeble evidencia que había utilizado para justificar la identificación; sin embargo, y a pesar de la casi unánime condena expresada por los críticos, hasta el día de hoy *Newsweek* sigue defendiendo esa

historia con la siguiente y débil defensa del interés público: «Reconocimos que existía un interés público en revelar algunos hechos básicos en relación con Bitcoin y en una mejor información para todos aquellos que pudieran invertir dinero en él.»[382] Incluso si hubiesen identificado a la persona correcta, las justificaciones éticas para abrir de par en par su vida ante la opinión pública parecían dudosas. El creador de Bitcoin ha expresado reiteradamente su deseo de permanecer anónimo; y lo que es más importante, sus acciones no han causado daños ni ningún perjuicio. Tampoco es en absoluto necesario conocer los detalles de la vida privada de este hombre para tomar «decisiones de inversión» sólidas sobre Bitcoin, como alegan los editores de *Newsweek*.

Por supuesto, al tratarse de una entidad pública y legalmente constituida, *Newsweek* puede ser demandada y, en 2014 Nakamoto parece que estaba explorando esta opción. Sin embargo resulta prácticamente imposible demandar por doxeo a un colectivo anónimo, a menos que antes el autor sea atrapado por el Estado o delatado por sus compañeros. Por el error y la violación de la privacidad cometidos por *Newsweek*, Nakamoto podría ser compensado con una enorme suma de dinero,[383] mientras que un agente de policía erróneamente doxeado recibió amenazas de muerte sin ninguna posibilidad de reparación.

La yuxtaposición de ambos casos pone de manifiesto algunas diferencias importantes en la rendición de cuentas de Anonymous, una entidad de protesta camuflada y una persona conocida o una institución pública. Pero otros ejemplos de inexactitudes y descuidos periodísticos han provocado un daño colateral mucho más inquietante que cualquier cosa de la que habitualmente Anonymous es capaz de llevar a cabo. Si bien un doxeo fallido cometido por Anonymous puede poner en peligro de manera imprudente a un puñado de individuos, la atribución errónea de la cual se hacen eco de manera acrítica los principales medios de comunicación puede ayudar y apoyar potencialmente determinadas decisiones que alteren el destino de naciones enteras. La mentira periodística más atroz e insidiosa de la última década es tan conocida que apenas si necesita mención: se produjo cuando *The New York Times* publicó un artículo que repetía acríticamente y como un loro la postura del gobierno estadounidense de que Saddam Hussein estaba almacenando armas de destrucción masiva. Como han señalado muchos críticos, este único artículo contribuyó a justificar una

guerra larga y terrible en Irak, una línea de actuación que ninguna demanda o respuesta de la sociedad civil podían aspirar a reparar.

Aunque este ejemplo puede parecer un caso atípico y excepcional, se pueden señalar muchos otros ejemplos cotidianos de traspiés periodísticos nocivos sustentados en alegaciones imprudentes, a menudo relacionados con el ámbito del propio activismo tecnológico. Muchos periódicos británicos han publicado historias que difaman a Edward Snowden como espía ruso, sin ni siquiera intentar presentar alguna prueba que justifique esa acusación. Julian Assange, acusado hasta la saciedad de ser irresponsable con sus filtraciones, fustigó a un periodista de *The Guardian* que publicó una contraseña interna sensible como encabezamiento de un capítulo en un libro que detallaba su colaboración con WikiLeaks. Según Assange, este hecho provocó «la descarga de cientos de miles de cables del Departamento de Estado en Internet, sin contar con las redacciones selectivas que se habían preparado cuidadosamente para ellos».[384] Assange había confiado la contraseña a un grupo selecto de periodistas con el acuerdo explícito de que el material al que se había accedido necesitaba ser cuidadosamente examinado antes de publicarse, para evitar el doxeo accidental de personas inocentes.

Por último, examinemos un caso relacionado directamente con Anonymous y al que hicimos referencia en páginas anteriores de este libro. En febrero de 2012, en el momento álgido de la popularidad de Anonymous, cuando los políticos polacos se colocaron la máscara de Guy Fawkes para mostrar su desacuerdo con un tratado comercial, una redactora de *The Wall Street Journal* llamada Siobhan Gorman describió a los hacktivistas como extremistas peligrosos. Anonymous «puede tener la capacidad en uno o dos años de provocar un apagón limitado mediante un ciberataque», escribió. La prueba era bochornosamente pobre y se reducía a una única frase: «El General Keith Alexander, el director, realizó esta evaluación durante unas reuniones celebradas en la Casa Blanca y en otras sesiones privadas, según personas familiarizadas con estas reuniones.»[385] La evidencia no era solo endeble sino que estaba tan alejada del comportamiento público de Anonymous que el artículo fue un rotundo fracaso. Pero si hubiese tenido éxito, podría haber invalidado los esfuerzos de todo un movimiento político para contribuir positivamente a una amplia variedad de causas sociales.

En ocasiones, Anonymous comete errores y los periodistas también. Pero cuando los errores los comete un periódico respetable, la respuesta habitual no consiste en denunciar a toda la profesión periodística o siquiera a la empresa editorial, sino más bien a un artículo concreto, al autor o al editor en cuestión. ¿Por qué debería ser diferente en el caso de Anonymous? Los errores particulares cometidos por Anonymous, *The New York Times* o *Newsweek* merecen todos ellos una dura crítica. Y esto es precisamente lo que ocurrió en el caso de la OpFerguson cuando TheAnonMessage divulgó un nombre que no era el correcto. Yo lo estaba observando en tiempo real en el IRC cuando este participante se conectó para hacer público el nombre del agente de policía. Era muy temprano y la mayoría de miembros de la operación estaban descansando o no se habían conectado. Habitualmente, las operaciones de doxeo se llevan a cabo de forma privada y esto estaba completamente fuera del guión porque TheAnonMessage actuaba de forma caprichosa sin consultarlo con el equipo principal, algo que normalmente sucede a puerta cerrada en los canales privados. Una vez que hubo divulgado el nombre— y fue evidente que se había equivocado—, casi todos los demás miembros de la operación se enfurecieron y arremetieron contra el Anon en cuestión. Uno de sus críticos más contundentes fue Crypt0nymous, un respetado creador de vídeos/medios en Anonymous, que lanzó una fuerte invectiva contra @TheAnonMessage en Twitter.[386] Crypt0nymous colgó docenas de mensajes sobre su mezquino e irresponsable trabajo que, según él, estaba motivado por un deseo de fama y gloria personales. Esta clase de censura y condena informales puede no ser lo bastante contundente como para corregir todos los errores pero, no obstante, los mecanismos informales de castigo modulan eficazmente las actividades futuras, en general para mejor.

La muestra de ejemplos extraída del campo del periodismo no pretende justificar las consecuencias perjudiciales que se derivan de las actividades de doxeo practicadas por Anonymous; con un error no se subsana otro. Es simplemente un recordatorio de que el mero hecho de trabajar bajo un régimen de transparencia no garantiza la rendición de cuentas ni un comportamiento responsable. De hecho, cuando periódicos respetables, como *The New York Times* o *The Wall Street Journal*, publican artículos o noticias con escasa evidencia que los sustente, las consecuencias pueden ser mucho más negativas que cuando las divulga un colectivo como

Anonymous; esos periódicos son considerados como vehículos de la objetividad y la verdad. Su reputación tiende a ser sólida y son difíciles de poner en cuestión. Las afirmaciones de Anonymous, en cambio, a menudo son recibidas, incluso por sus propios partidarios, con cierto grado de escepticismo.

En efecto, es encomiable que Anonymous señale los prejuicios y enfoques inherentes a todos los entornos informativos, ya sea que se deban a limitaciones cognitivas, al exceso de información, a los prejuicios inherentes que son parte integral de la producción de conocimiento, a una información imperfecta o directamente a la manipulación de la información. El hecho de que sepamos que Anonymous es falible es valioso en sí mismo. Ellos no reivindican la objetividad. No afirman ser justos y equilibrados, sino simplemente que son activistas que hacen todo lo posible por ser traviesos. Por lo tanto, sus fallos quedan inmediatamente bloqueados para provocar un daño excesivo porque en primer lugar nadie espera que sus acciones sean un 100 por cien correctas todo el tiempo, a diferencia de lo que ocurre con una organización respetable como *The New York Times*.

Aun así, las comparaciones entre Anonymous y el periodismo solo pueden llegar hasta este punto. El alcance de la actividad de la que participa Anonymous, un movimiento político orientado hacia la acción, es mucho mayor que el de los medios de comunicación, dedicados exclusivamente a divulgar información. Mientras que, en muchos casos, Anonymous es responsable, mediante seudónimos, como grupo operativo, en otros casos sus manifestaciones más radicales y de acción directa dependen de la confidencialidad y el anonimato incluso en relación con otros Anons. Las actividades de acción directa más arriesgadas, en particular, son a menudo activadas y promovidas en nichos reservados, como las «élites dentro de élites» descritas anteriormente en este libro. Otra aplicación de la confidencialidad apunta menos a la seguridad y más a mantener cierto tipo de armonía social interna: Anons excluye a aquellos que participan de comportamientos sociales ostentosos, exigiendo a menudo que la identidad personal sea ocultada no simplemente por razones de seguridad personal sino más bien para contener el ego personal.

Estos dos registros de oscurantismo aportan ejemplos de lo que el experto en comunicación Jack Bratich elogia como «confidencialidad popular menor», valiosa por «proporcionar un exhibidor a una política

basada en la identidad y la representatividad».[387] A menudo, sugiere Bratich, los intentos realizados por los movimientos sociales para exigir visibilidad y representación funciona menos para promover sus demandas políticas y más para volverlas legibles a los mecanismos estatales de cooptación o rechazo.[388] Dejando constancia de que el Estado «aborrece calquier máscara que no sea suya», sugiere que existe una enorme distancia en la manera en que el Estado “demoniza” las máscaras que utilizan sus ciudadanos al tiempo que se niega siempre a renunciar a las propias. A resultas de ello, Bratich sostiene que las actividades izquierdistas deberían reservar un lugar limitado pero importante a la confidencialidad. Cuando los activistas critican toda forma de confidencialidad en el activismo, están fortaleciendo inadvertidamente el poder del Estado; su transparencia demuestra todas sus vulnerabilidades para que un oponente enmascarado las explote o coopte desde una posición ventajosa segura.

¿Qué ganan los activistas al confiar en formas de confidencialidad menores y limitadas, sobre todo cuando están reforzadas por una ética de la confusión utilizada para promover el igualitarismo? Y ¿es posible que el empleo de la confidencialidad pueda ser éticamente justificada cuando la utilizan grupos políticos activistas débiles, pero rotundamente condenada cuando la utilizan aquellos —Estados y poderosos actores económicos— que ya ostentan una ventaja o el monopolio del poder? Cuando la confidencialidad se utiliza por los Estados no solo de manera instrumental sino como una norma de funcionamiento general y en constante expansión —como es concretamente el caso de las agencias de inteligencia dotadas con recursos financieros y técnicos aparentemente ilimitados— a menudo sus efectos puede ir contra el interés público. [389] La confidencialidad, de otra parte, proporciona a los activistas que disponen de recursos escasos, como es el caso de Anonymous, la capacidad de golpear a los poderosos. Nivela el campo de juego. Cuando se utiliza de una manera restringida, el encubrimiento puede alterar positivamente el panorama político, posibilitando condiciones estructurales capaces de activar la acción basada en principios, en lugar de la deliberación y la comunicación basadas en ellos; también puede constituir una forma de acción directa en el pleno sentido de la palabra. Tal como lo ha expresado Julian Assange, «la criptografía es la forma más perfeccionada de acción directa no violenta».[390]

La inacción política tiene costes concretos. Cuando la gente privilegia la política liberal del debate, la reforma y la publicidad por encima de la participación directa en el cambio, resulta difícil entender de dónde, exactamente, se espera que llegue el cambio cuando el gobierno opta por no escuchar. Nuestra sociedad aboga por la transparencia y el debate ciudadano. A menudo se considera estos mecanismos como la manera preferida de ejercer una presión política capaz de impulsar a los responsables políticos y a los legisladores a que inicien el cambio. Pero, aunque hacer que la información esté disponible y abierta al debate público es algo innegablemente valioso, para que la información se convierta de verdad en algo políticamente importante a veces necesita ser práctica, necesita ser moldeada en forma de una exigencia que no puede ser ignorada.[391]

La desobediencia civil es una vía para conseguirlo y su ejercicio puede servir como un modelo que ofrece a un número mayor de participantes —aquellos a los que la política liberal convencional no atiende o no les ofrece una voz para expresarse, o las minorías acalladas con una convención normativa irreflexiva— un camino a través del cual contribuir directamente al proceso político. Como ha dicho Robin Celikates, un teórico político que trabaja sobre la desobediencia civil, «la forma de acción política esporádica, informal, y extra o anti institucional también permite que los ciudadanos protesten y participen cuando —como sucede a menudo en las democracias representativas— los canales de acción y comunicación institucionales regulares y oficiales les están vedados o son ineficaces para conseguir que sus objeciones sean atendidas».[392]

Se puede objetar el empleo de la desobediencia civil por parte de una minoría. Al fin y al cabo, ¿es posible que su opinión sea inusual precisamente porque no es deseable? Pero este es un análisis engañoso. La desobediencia civil, incluso cuando funciona, solo sirve para llamar la atención sobre una postura concreta, una que debe alinear a un número mayor de personas para construir una causa más importante si su propósito es cambiar el consenso general. Las posturas asumidas por individuos como Chelsea Manning, Jeremy Hammond y Edward Snowden eran poco conocidas hasta que sus valientes actos permitieron que su política fuese conocida y, de este modo, emulada por todos aquellos que coincidían con ella. (Existe probablemente al menos otra persona que está filtrando

documentos de la NSA a varias plataformas de publicación,[393] y es probable también que Phineas Fisher se sintiese inspirado por los hackeos de Anonymous contra empresas de seguridad.) La valentía de esta naturaleza, ya sea anónima o no, desafía a otros a enfrentarse y, en ocasiones, a desprenderse de su complacencia. En otras palabras, la desobediencia civil crea un entorno donde pueden prosperar movimientos sociales de base más importantes.

Anonymous representa un ejemplo perfecto del funcionamiento de esta lógica. Los participantes que doxean, hackean o dosean son minoría. Pero al llevar a cabo estas acciones contribuyen a animar a los espectadores y a otros participantes, incluso a aquellos que no están de acuerdo con sus tácticas o sus resultados.[394]

Sin embargo, la cuestión relacionada con la rendición de cuentas por parte de Anonymous es planteada nuevamente por los críticos en este terreno, a menudo críticos que defienden obstinados el uso de la desobediencia civil por parte de otros movimientos sociales. La desobediencia civil, afirman, carece de legitimidad si no lleva el sello de nuestra identidad legal, si no está legitimada por el riesgo de sufrir un castigo. Pero tal como ha argumentado de manera convincente Molly Sauter, esta concepción de la desobediencia civil es tan estrecha (y limitada) como históricamente específica. Se trata de una concepción, insiste Sauter, «profundamente arraigada en conceptos del martirio cristiano y la superioridad moral que tiene el desobediente civil no violento sobre sus adversarios... al insistir en que los activistas políticos en la red se exponen a la a menudo extremadamente punitiva acción del Estado asegura que solo aquellos que sustentan las concepciones más extremas y tienen menos que perder (es decir, aquellos con la menor inversión en la sociedad) participarán en estas acciones».[395]

Mientras Anonymous continúa planteando exigencias al Estado, buscando erradicar la corrupción y vinculándose con otros activistas con el fin de proporcionar ayuda para las grandes y pequeñas luchas políticas, actúa para descolonizar hábitos de subjetividad profundamente arraigados: se atreve a avanzar hacia un bien colectivo sin la necesidad del reconocimiento personal y la promoción de una marca personal. Después de todo, muchos de sus participantes son ciudadanos capaces, respetuosos con la ley que podrían, si quisieran, buscar cierto grado de gloria pública y

personal a cambio de sus contribuciones. En cambio, ellos insisten en el "derecho a la opacidad", como lo formuló Edouard Glissant. [396] El enmascaramiento, considerado a menudo solo en términos negativos —como una forma de rehuir u ocultar la responsabilidad— puede permitir también una ética de la interacción y de estar-en-el-mundo positiva y constructiva que contrarreste los intereses estatales, corporativos y coloniales. De hecho, este derecho encarna una serie de negativas desafiantes basadas en principios; la negativa a permitir que el Estado vigile a sus ciudadanos; la negativa a permitir que las corporaciones conviertan las comunicaciones personales en un beneficio económico o manipulen sus deseos personales; la negativa a aprovecharse de la mano de obra del otro; la negativa, en esencia, a impedir que una idea fecunda —que somos y podemos ser anónimos— se marchite.

Julio de 2015

Agradecimientos

Aunque un único concepto esté abocado al fracaso en su intento de transmitir la vasta e intrincada geografía construida por los activistas de Anonymous, al escribir este libro descubrí que regresaba sistemáticamente a un tropo dominante concreto: el laberinto. Cada intento de atravesar, entender o describir un estado determinado lo corrompía forzosamente, añadiendo más contribuciones entrópicas que aseguraban una experiencia diferente para cualquiera que quisiera participar en ella o incluso simplemente observar. De modo que, al final, investigar y escribir sobre Anonymous resultó ser una empresa apasionante pero agotadora. Pasé años reuniendo demasiado material, tratando de construir mi propio laberinto que me permitiese trazar un rumbo a través del de ellos. Pero cuando me propuse desenredar el enmarañado ovillo para encontrar una salida a los secretos, rumores, historias y conversaciones que había conseguido reunir y proporcionarles alguna narrativa lúcida y coherente, comprendí horrorizada que el material, fino como el de la telaraña, se deshacía entre mis dedos. Estaba perdida en las regiones abisales, entre laberintos, sin ninguna orientación y sin salida. Afortunadamente, un montón de amigos, colegas, desconocidos y Anons me ayudaron a encontrar el camino, impulsándome hacia adelante en mi viaje y contribuyendo a su manifestación final en forma de libro.

Este proyecto me llevó mucho tiempo. Los comienzos se remontan a la beca Killam de Investigación Posdoctoral, que disfruté en la Universidad de Alberta en el período 2006–2007, y a una afortunada presentación al Dr. Stephen A. Kent, quien, en su trabajo como profesor de sociología, cuida el mayor archivo con material sobre la Cienciología que existe en el mundo. En medio de un invierno espantosamente helado, me sumergí en ese archivo

con la esperaza de salir a la superficie con un breve proyecto colateral histórico que describiese un caso que entre los geeks se conoce como “Cienciología versus Internet”. Al estar más acostumbrada a entrevistar a personas que a encontrar el sentido a pilas de documentos (en este caso, muy extraños), Kent me guió afortunadamente y con gran amabilidad a través de las confusas, fascinantes y por momentos inquietantes vísceras de una organización a la que a muchos geeks les encanta aborrecer.

En enero de 2008, mi proyecto histórico dio un salto hasta el presente cuando, en el proceso de elegir como objetivo de sus ataques a la Iglesia de la Cienciología, Anonymous experimentó la amplia y sorprendente metamorfosis de temibles bromistas a fervientes manifestantes. Estaba enganchada. Me pareció absolutamente natural seguir a estos locos sombrereros y ver qué surgía de su audaz e inesperada incursión en la cultura de la protesta; y es evidente que algo surgió. En aquella época me había instalado nuevamente en Nueva York y descubrí un portal físico hacia Anonymous a través de la bulliciosa célula local que me acogió en sus protestas mensuales. Yo, a mi vez, recibí a miembros de esa célula en mi clase, donde junto con mis estudiantes nos beneficiamos de sus elocuentes disertaciones sobre la importancia política de Anonymous y sus payasadas teatrales demostrando el lulz. Little Sister, Sethdood y Matthew “PokeAnon” Danziger se reunieron conmigo en varias ocasiones y se revelaron como unos animados interlocutores. Los últimos dos incluso aceptaron realizar entrevistas formales. También tuve el placer de establecer una estrecha relación con Chanology Dublín y otros Anons irlandeses; ellos fueron algunos de mis maestros más intrépidos. Crucé el océano en numerosas ocasiones para recurrir a ellos, y para mi tercer viaje en un período de tres años ya estaba claro que algunos, sobre todo Pete, David, Firefly y Donncha, se habían convertido en algo más que fuentes, se habían convertido en amigos. Espero mantener otros intercambios con ellos en el futuro.

En 2010, cuando Anonymous penetró en la conciencia pública con su campaña digital de acción directa, protestando contra el bloqueo bancario impuesto a WikiLeaks, yo me encontraba de manera fortuita disfrutando de un período sabático en un santuario: el Instituto de Estudios Avanzados en Princeton. El ritmo agotador de la actividad que luego llegó como un alud desde la red de AnonOps habría sido prácticamente imposible de seguir si

no hubiese sido por el exceso de tiempo del que pude disponer. Las conversaciones con dos colegas de mi grupo, Manu Goswami y Tanya Erzen, contribuyeron a moldear mi visión del tema. El antropólogo Didier Fassin demostró ser un mentor inspirador, cuya ilimitada voluntad de compartir opiniones y sugerencias se confirmó una vez más después de que yo presentase un trabajo sobre Anonymous en un taller reciente sobre etnografía pública realizado en el IAS.

Con la llegada de 2011 me entregué a tiempo completo al siempre cambiante laberinto de Anonymous. En algunos momentos deambulando sin ningún propósito o dirección precisos y, en otros, firmemente decidida a cumplir una misión, hablé con docenas de participantes, beneficiándome de su tiempo, experiencias, reflexiones y críticas. Os agradezco a cada uno de vosotros y lamento mi incapacidad para recordar e incluir todos vuestros nombres, ya sean reales, falsos o seudónimos. Algunos de ellos merecen una mención especial por haber ido más allá de lo que les pedí en su deseo de guiarme. En una fase temprana, onTrivette, meddle y n0pants hablaron conmigo personalmente y, al hacerlo, me abrieron numerosas puertas. Encontré hogares acogedores en #reporter, #freedommods y finalmente en #cabincr3w, donde las conversaciones se prolongaban durante horas y eran siempre animadas y esclarecedoras. Con el paso del tiempo, un puñado de otros amigos me señaló diferentes caminos para la reflexión. Anonymous9 — rebosante de energía— fue una persona inagotablemente útil en mi investigación. Este libro, al menos en esta forma, simplemente no habría sido posible sin él. M0rpeth fue probablemente el primero de un grupo de insiders que me imploró que dejase de beber Kool-Aid; sus incisivas críticas de las estructuras de poder emergentes hicieron que me resultase más fácil intuirlas y, al hacerlo, entender las numerosas cepas de crítica interna existente en Anonymous. Blackplans, una presencia consistente que abarca diferentes épocas y escenarios, se mostró versado y ocurrente en relación a Anonymous y los hackers (por no mencionar la vida en general). Andrew Auernheimer, sin duda lejos de ser anónimo, o un fan de Anonymous, me enseñó mucho sobre troleo, a menudo a través de sus argumentos y afirmaciones sobre el tema, pero afortunadamente nunca me troleó a mí. Muchos otros dedicaron bastante tiempo a chatear conmigo, incluidos c0s, AnonyOps, Barrett Brown, evilworks, q, mr_a, sharpie, Katanon, shit-storm, owen, Avunit, emmi, Jackal, p0ke, crypt0anonymous,

Nicole Powers, Nixie, Commander X, JMC, paperspl x, Lauri Love, y otros que permanecerán en el anonimato.

Con el tiempo (y debido a una sucesión de arrestos), las circunstancias de mi investigación cambiaron en igual medida que la percepción pública de los temas tratados. Muchos Anons han soportado difíciles batallas legales y penas de prisión. Teniendo en cuenta lo complicadas que se volvieron sus vidas, me siento aún más agradecida de que me hayan dedicado su tiempo. El libro sencillamente no se podría haber terminado sin la generosidad y la sagacidad de Jeremy Hammond, Mustafa Al-Bassam, Donncha O'Cearbhaill, Darren Martyn y Mercedes Haefer, cada uno de los cuales dedicó horas a responder series interminables de preguntas, a veces repetitivas. Chris Weatherhead y Jake Davis también se reunieron conmigo personalmente para compartir muchas de sus experiencias; Ryan Ackroyd, con quien comencé a relacionarme hace muy poco tiempo, hizo meditadas reflexiones sobre la "Máquina del odio de Internet" y los informadores.

En el curso de la investigación se me podía encontrar chateando con periodistas y cineastas que, al igual que yo, dedicaban una enorme cantidad de tiempo y duro trabajo a intentar descifrar el puzzle de Anonymous. Su presencia era siempre bienvenida, las tertulias y el intercambio de notas de nuestras respectivas investigaciones demostraron ser a la vez cómicamente tranquilizadoras y profesionalmente valiosas. Las conversaciones con Quinn Norton, Asher Wolf, Steve Ragan y Brian Knappenberger fueron decisivas para la idea que tenía de Anonymous. Steve Ragan merece también una mención especial por compartir conmigo sus cosas de un modo generoso; la mayoría de los periodistas son mucho más cautelosos con sus posesiones. La película de Knappenberger y el fascinante relato de Parmy Olson sobre Anonymous y LulzSec fueron recursos muy valiosas para este proyecto.

En 2013, un numeroso grupo de colegas leyó un par de los primeros capítulos y aportó profundas observaciones: Danielle Citron, Nathan Schneider, Jonathan Sterne, Darin Barney, Christine Ross, Carrie Rentschler, Sandra Hyde, Michael Ralph, Whitney Phillips y Chris Kelty. Con el correr de los años he disertado extensamente sobre Anonymous y resultaría imposible hacer balance de todas las generosas respuestas que recibí; sin embargo, cabe destacar los comentarios de Paul Eiss, Angela Zito, Faye Ginsburg, Haidy Geismar, Daniel Miller, Alberto Sánchez y Bob

Rutledge.

En la Universidad McGill tengo la fortuna de ocupar un cargo concebido para permitir mi compromiso tanto en la divulgación como en la escritura; estoy profundamente agradecida al generoso donante que proporciona su financiación. El ambiente en McGill ha resultado muy estimulante y me siento especialmente agradecida a todos los participantes Bits, Bots y Bytes por su contribución a un foro de investigación y al intercambio académico que se ha convertido en uno de los hitos de mi mes. Dos de sus miembros, Scott Kushner y Elena Razlogova, leyeron e hicieron inteligentes aportaciones a un material adicional compartido fuera de la reunión. Maya Richmond, mi estudiante de licenciatura e infatigable asistente de investigación has perseguido con éxito hasta la última pizca de material que le pedí al tiempo que también me proporcionaba agudos comentarios con respecto a hackers y embaucadores. Caroline Habluetzel, que recibió un doctorado de nuestro departamento, también aportó a la investigación una ayuda valiosa y meticulosa, y eso mientras luchaba contra el cáncer. Caroline falleció en mayo de 2013 y la echaremos mucho de menos. Mi curso universitario, “Technological Underworlds” (submundos tecnológicos) recibió un borrador preliminar de los cinco primeros capítulos para que los leyeran, lo que dio como resultado preguntas fascinantes y la detección de varios problemas. Darcie DeAngelo fue más allá de lo solicitado para incluir extensos comentarios sobre el texto. Molly Sauter estaba acabando su propio libro —*The Coming Swarm: DDOS Actions, Hacktivism, y Civil Disobedience on the Internet*— en la misma época y su lectura del manuscrito resultó fundamental y a la vez fascinante mientras yo examinaba la ética de la acción directa digital.

Escribir un libro para una audiencia popular mientras te mantienes fiel a una serie de detalles complejos, esotéricos, técnicos y jurídicos representa un formidable desafío. Acudí al consejo de numerosos expertos para asegurarme de que no estaba tergiversando estos matices. Orin Kerr, Marcia Hoffman, Ahmed Ghappour y Andrés Guadamuz se encargaron de leer las secciones legales. Muchos tecnólogos y hackers siempre dieron cumplida respuesta a mis numerosas preguntas: David Mirza, Chris Soghoian, Dino A. Dai Zovi, Chris Wysopal, Space Rouge, James Atkinson, Patrick Gray, Dan Guido, Morgan Marquis-Boire y Brian Martin. Entretanto, los periodistas Kim Zetter y Ted Bridis se encargaron de aclararme unas

cuantas dudas que tenía acerca de los hackers y la política del FBI respecto de los informadores. Cualesquiera inexactitudes que aún se conserven en el texto serán producto de mi incapacidad para seguir la excelente guía de estos asesores.

A los miembros de mi familia debo agradecerles el haber soportado las consecuencias negativas de la redacción de un libro, los Anderson se mostraron pacientes y amables cuando las últimas tres temporadas de vacaciones no me vieron tan presente como a todos los demás. Mi padre, un incansable aliado de mi trabajo, se aseguró de que sus amigos, la mayoría de ellos ya retirados, aprendiesen algo importante sobre Anonymous. Mi perro *Roscoe*, con su divertido diente torcido, se encargó todos los días de sacarme del escritorio para asegurarse de que tomara los descansos necesarios lejos del texto.

Finalmente, hay tres personas cuyo sello se puede encontrar en todas partes en este libro y que lo han leído de cabo a rabo, dos de ellas más de una vez. Mi compañero Micah Anderson, que pasa sus días (y sus noches con demasiada frecuencia) dirigiendo una ISP que protege la privacidad, es un talentoso escritor. Él leyó los primeros capítulos y me señaló el hecho de que debía ser más intensa y descriptiva si mi intención era que fuese un libro más popular que académico. Sus lecturas posteriores de cada uno de los capítulos siempre dieron lugar a comentarios o revisiones útiles. Micah sin duda regó con gasolina todos mis intentos humorísticos antes de encender una cerilla y avivar el fuego con chistes de su propia cosecha. Algunos de ellos eran simplemente demasiado locos e imaginativos y tuve que apagar las llamas, pero después las cosas mejoraron notablemente. Estoy profundamente agradecida de que desee formar parte del proceso creativo y de que me haya soportado mientras escribía dos libros de forma consecutiva, algo que nunca jamás volveré a hacer.

En parte debido al consejo de Micah —y en parte por mi propia tendencia a explicarlo todo— me excedí totalmente con la escritura. Dos personas estaban listas para contenerme, señalar mis contradicciones, ayudarme a reducir el manuscrito a un tamaño razonable y, en general, hacer todo lo que estuviese en su mano para que este libro fuese mejor.

En primer lugar, mi asistente de investigación Matt Goerzen, que es también mi estudiante de máster y un artista talentoso y extravagante especializado, entre otros temas, en el anonimato, fue un editor de primera

categoría. Formado como periodista, Matt es además un hábil escritor dotado para añadir un toque de gracia y claridad a cualquier prosa que se cruce en su camino. Puesto que ha estudiado profundamente y completado numerosas investigaciones sobre las culturas del anonimato en la red, sus comentarios eran siempre agudos y perspicaces. Este libro es mucho más sólido gracias a su generosa disponibilidad a compartir su sabiduría. Le estaré eternamente agradecida de que asumiera el papel de mi guía e interlocutor más fiable, y solo espero que pueda pagar mi deuda en mi carácter de supervisora de su tesis de master.

Cuando consideraba posibles editores para el libro, mi idea era encontrar a uno que me ayudase a alcanzar el equilibrio correcto entre análisis y accesibilidad; Verso se presentó de inmediato como el candidato número uno y ha sido para mí un placer trabajar con todo el equipo de la editorial, incluidos Mark Martin, Colin Beckett, Jennifer Tighe y Jacob Stevens. Me siento especialmente agradecida por haber podido trabajar con Andrew Hsiao. Cuando el libro creció hasta alcanzar un tamaño inaceptable, confieso que temí las estrictas medidas que Andrew podía tomar para recortar el manuscrito. Mientras me temía lo peor, su consejo demostró finalmente ser excelente y a la vez específico, consiguiendo que el proceso de poda fuese mucho menos doloroso de lo que pudo haber sido. Examinó el manuscrito con lupa; se mostró minucioso con los pequeños detalles de la redacción, tuvo en cuenta el valor de mis argumentos y tomó distancia para identificar las secciones, las oraciones e incluso los capítulos donde era necesario rasurar y cortar. Hubo momentos en los que, si fuese posible abrazar a alguien a través del correo electrónico, él habría sido en muchas ocasiones el destinatario de ese abrazo. También disfruté plenamente de nuestras conversaciones sobre edición y política y espero mantener muchas más en el futuro.

Por último, me gustaría agradecer a todos los activistas y bromistas enmascarados por representar su obra ferozmente épica y haberme dado la oportunidad de escribir sobre ella.

Nota sobre las fuentes

Al presentar una etnografía popular de Anonymous, este libro se basa en gran medida en la convención periodística y las metodologías de búsqueda de fuentes. Muchos lectores se preguntarán cómo es posible verificar la información contenida en estas páginas si tenemos en cuenta que las mentiras, el engaño y la invención son las herramientas del oficio, a menudo utilizadas con orgullo por todos aquellos que operan bajo el manto de Anonymous. Pero si bien algunas de las anécdotas incluidas siguen siendo inverificables, o están acompañadas simplemente de registros de chat, complementan una narrativa objetiva que ha sido posible gracias a registros legales. De hecho, este libro nunca habría existido si no fuese por el desenmascaramiento de muchos de los participantes debido a su detención y juicio, y a los caudales de cuidadosa (y en ocasiones problemática) información hecha pública por las fuerzas de la ley con este fin. Además, aunque el anonimato, por su propia naturaleza, permite que los individuos se pronuncien contra instituciones poderosas y las desafíen, luego de ser arrestados y condenados muchos participantes disfrutan de pronto de una clase diferente de libertad: la capacidad de hablar honestamente sobre sus identidades y experiencias personales como individuos, alejados de un seudónimo colectivo o protector. El acceso a los registros y, sobre todo, a los documentos de los tribunales me ha permitido certificar muchas de las afirmaciones hechas por Anons y sus colegas antes de su arresto (en la gran mayoría de los casos lo que me habían dicho resultó ser verdad).

Los extensos registros de chat citados en este libro proceden de numerosas fuentes: de canales públicos de IRC, de registros publicados en la red por Anonymous, de registros privados que me habían entregado y,

finalmente, de registros presentados como pruebas ante el tribunal y filtrados a los periodistas. En los casos en los que no existía ningún documento, he tratado de entrevistar a múltiples participantes y de confiar, siempre que era posible, en relatos publicados por respetadas figuras de los medios de comunicación. Es una triste realidad que muchos relatos y participantes fascinantes no están incluidos en estas páginas ante la imposibilidad de ser comprobados más allá del rumor. Puesto que muchas de las figuras incluidas en este libro son hoy muy conocidas de la opinión pública —y sobre las que se ha escrito extensamente— no he cambiado sus nombres ni tampoco sus seudónimos, excepto en los casos en los que no hacerlo podía haber supuesto una amenaza para la persona en cuestión.

Este libro debe leerse como una colección de experiencias y reflexiones personales. Aunque abordo acontecimientos importantes y puntos de inflexión históricos y trato de ser inclusiva con respecto a perspectivas múltiples, y en ocasiones hasta conflictivas, en el seno de Anonymus operan muchas más cosas que las que constan en estas páginas.

Notas del traductor

En este libro aparecen muchos términos propios del universo de la piratería informática que he optado por dejar en inglés. Muchos de ellos son los que llevan el sufijo *fag*, versión abreviada de la palabra *faggot* que, en el habla popular estadounidense, hace una referencia peyorativa a los homosexuales de ambos géneros y, en una acepción más amplia, a una persona repelente o desagradable. El lector se encontrará, entonces, con términos como *newfag*, *namefag*, *moralfag* o *liderfag* en los que ese sufijo cumple una función peyorativa de la palabra que acompañan y que serían, en una traducción casi literal, "nuevos maricones", "maricones de los nombres", "maricones de la moral" o "líderes maricones".

Introducción: Y ahora habéis captado nuestra atención

* LOL es un acrónimo inglés que significa Laughing out loud, que se traduce como "reírse en voz alta o a carcajadas". (N. del t.)

** Objetos virtuales que componen el mobiliario de Habbo, furniture, que sirven para decorar las salas. (N. del t.)

*** Juego de palabras con el término dick en sus acepciones vulgares de capullo y polla. (N. del t.)

**** Pequeños donuts en forma de bola típicos de Canadá. (N. del t.)

Notas del traductor

Capítulo 1. Sobre trols, embaucadores y el lulz

* La metilendioxipirovalerona (MDVP) es una droga psicoactiva que posee potentes efectos alucinógenos y estimul

** *God's War* es una trilogía escrita por Kameron Hurley y protagonizada por una ex asesina del gobierno convertida en caza recompensas y a la que pagan para atrapar a terroristas y desertores. (N. del t.)

*** En la comunidad hacker, un sombrero gris hace referencia a un hacker talentoso que, aunque pueda actuar ilegalmente, lo hace con buenas intenciones. (N. del t.)

**** El emo es una subcultura urbana originada en la década de 1980 en Washington D.C. alrededor del género musical emo ("emotional hardcore"), un subgénero del *hardcore punk*. En la cultura hacker, todo lo emo es odiado y tomado como objeto de troleo. (N. del t.)

***** Un phreak es una persona que encuentra una deficiencia en el sistema telefónico y consigue así un uso barato o gratuito del teléfono. (N. del t.)

Notas del traductor

Capítulo 2. Proyecto Chanology: vine por el Lulz pero me quedé por la indignación

* Botnet es un término que hace referencia a un conjunto o red de “robots informáticos” o “bots”, que se ejecutan de manera autónoma y automática. (N. del t.)

** Lulz tipo rugido (N. del t.)

*** phpBB es un sistema de foros gratuito basado en un conjunto de paquetes de código programados en el popular lenguaje de programación web PHP. (N. del t.)

Notas del traductor

Capítulo 3. Las armas de los Geeks

* *El club de la lucha*, novela de Chuck Palahniuk en la que se basaría una popular película del mismo título, protagonizada por Edward Norton, Brad Pitt y Helena Bonham Carter (N. del t.)

Notas del traductor

Capítulo 8. LulzSec

* Puertorriqueño de Nueva York (N. del t.)

** Organización sin ánimo de lucro que sirve de asociación público-privada entre empresas estadounidenses y el FBI (N. del t.)

*** LED pegada a una batería de litio de 2032 3 volt y a un imán de enorme potencia. (N. del t.)

Notas del traductor

Capítulo 10. El deseo de un secreto es ser revelado

* Personaje del cómic *X-Men* (Nota del t.)

Notas del traductor

Conclusión: El *Aurora*

* *E pluribus unum* es uno de los primeros lemas nacionales de Estados Unidos y significa “De muchos uno” o “Unidad en la diversidad” y está incluido en el Gran Sello de ese país. (N. del t.)

Notas del traductor

Epílogo: El estado de Anonymous

* Así se denomina a menudo al escenario con el que se encuentran las agencias de la ley en Estados Unidos cuando los cambios en los servicios y tecnologías de la comunicación les impiden interceptar y acceder a la información de conformidad con órdenes emitidas por un tribunal. (N. del t.)

NOTAS

Introducción. "Y ahora habéis captado nuestra atención"

1 “Querida Fox News,” vídeo de YouTube, publicado por dearfoxnews, 29 de julio, 2007, última visita 8 de julio, 2014, disponible en http://www.youtube.com/watch?v=RFjU8bZR19A.

2 Esta cita corresponde a una charla en una clase.

3 “Mensaje a la Cienciología,” vídeo de YouTube, publicado por Church0f cienciología, 21 de enero, 2008, última visita, 4 de julio, 2014, disponible en http://www.youtube.com/watch?v=JCbKv9yiLiQ.

4 Siobhan Gorman, “Power Outage Seen as a Potential Aim of Hacking Group,” online.wsj.com, 21 de febrero, 2012.

5 Sam Biddle,“ “No, Idiots, Anonymous Isn’t Going to Destroy the Power Grid”, gizmodo.com. 21 de febrero, 2012.

Capítulo 1. Sobre trols, embaucadores y el lulz

6 Danielle Keats Citron, Hate 3.0: *The Rise of Discriminatory Online Harassment and How to Stop It* (Cambridge, MA: Harvard University Press, de próxima publicación); Danielle Keats Citron, “Cyber Civil Rights,” *Boston University Law Review*, vol. 89 (2009).

7 Para una detallada crítica de la CFAA y recomendaciones para su reforma, consúltese http://www.eff.org/issues/cfaa.

8 Tom McCarthy, “Andrew Auernheimer’s Conviction over Computer Fraud Thrown Out,” theguardian.com, 11 de abril de 2014.

9 Joseph Carey, post en Twitter, 22 de julio de 2013, 10:22hs., http://twitter.

com/JDCareyMusic/status/35936 2756568285184.

10 weev, “I am weev. I may be going to prison under the Computer Fraud and Abuse Act tomorrow at my sentencing. AMA.”, reddit, 17 de marzo de 2013, última visita, 21 de mayo de 2014, disponible en http://www.reddit.com/r/IAmA/comments/1ahkgc/i_am_weev_i_may_be_going_to_prison_under_the/c8xgqq9.

11 Daniel Bates, “Standing by Her Man: Strauss-Kahn’s Wife Puts Her Mansion Up as Collateral to Get Him out of Jail and She’s Paying the Rent at His ‘Golden Cage’”, *dailymail.co.uk*, 21 de mayo de 2011.

12 “Lulz”, Encyclopedia Dramatica, última visita, 23 de mayo de 2012, disponible en http://encyclopediadramatica.es/Lulz

13 Para referencias anteriores al “lulz” en el sitio de Jameth’s LiveJournal, consúltese http://web.archive.org/web/20021102 004836/ http://www.livejournal.com/users/jameth (última visita, 22 de mayo de 2014).

14 Whitney Phillips, “LOLing at Tragedy: Facebook Trolls, Memorial Pages and Resistance to Grief Online,” *First Monday* vol. 16, n. 12 (2011).

15 Muchas de estas ideas se exploran deliciosamente en el majestuoso relato de Lewis Hyde *Trickster Makes This World: Mischief, Myth, and Art* (Nueva York: Farrar, Straus y Giroux, 1998).

16 Ibid., p. 9

17 Alex R. Galloway y Eugene Thacker, *The Exploit: A Theory of Networks* (Minneapolis, MN: University of Minnesota Press, 2007).

18 Phil Lapsley, *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell* (Nueva York: Grove Press, 2013), 226.

19 Steven Levy, *Hackers: Heroes of the Computer Revolution—25th Anniversary Edition* (Sebastapol, CA: O’Reilly Media, 2010).

20 Adam L. Penenberg, “A Private Little Cyberwar”, forbes.com, 21 de febrero de 2000.

21 “Biography of u4ea,” soldierx.com, última visita, 21 de mayo de 2014, disponible en https://www.soldierx.com/hdb/u4ea.

22 Marco Deseriis, “‘Lots of Money Because I Am Many’: The Luther Blissett Project and the Multiple-Use Name Strategy”, in *Cultural Activism: Practices, Dilemmas and Possibilities* (Amsterdam: Rodopi, 2011), 65–93.

23 Trond Lossius, “/55\[Fwd: [max-msp] it’s over]”, /55\ lista de correo, 15 de enero de 2001, última visita, 21 de mayo de 2014, disponible en http://www. bek.no/pipermail/55/2001-January/000102.html. Un buen ejemplo del arte de Nezvanova se puede encontrar en http://www.nettime.org/Lists- Archives/nettime-bold-0009/msg00073.html (última visita, 21 de mayo de 2014).

24 Lee Knuttila, “Users Unknown: 4chan, Anonymity and Contingency”, *First Monday*, vol. 16, n. 10 (Octubre de 2011).

25 “La máquina del odio de Internet” fue una frase empleada en un programa local de Fox News en Los Ángeles en 2007 para describir a Anonymous. El grupo convirtió rápidamente la frase en un popular meme.

26 Phillips, “LOLing at Tragedy.”

27 David Graeber, “Manners, Deference, and Private Property in Early Modern Europe” *Comparative Studies in Society and History*, vol. 39 (Octubre de 1997): 694–728.

28 Christopher Kelty,*Two Bits*:*The Cultural Signifcance of Free Software* (Durham, NC: Duke University Press, 2008)

Capítulo 2. Proyecto Chanology: vine por el Lulz pero me quedé por la indignación

29 XENU TV, “The Story Behind the Tom Cruise Vídeo Link”, Why We Protest, 27 de julio de 2013, última visita, 23 de may de 2014, disponible en http://whyweprotest.net/threads/the-story-behind-the-tom-cruise- video-leak.93170/page-3#post-1875660.

30 “The Cruise Indoctrination Vídeo Scientology Tried to Suppres”, gawker.com, 15 de enero de 2008, última visita, 11 de julio de 2014.

31 L. Ron Hubbard, “Scientology Technology,” *The Auditor*, n. 41 (1968).

32 XENU TV, “The Story Behind the Tom Cruise Vídeo Link”.

33 “Código de conducta”, vídeo de YouTube, publicado por ChurchOfScientology, 1 de febrero de 2008, última visita, 23 de mayo de 2014, disponible en http://www.youtube.com/watch?v=-063clxiB8I.

34 Cain, “Hal Turner Raid Planned for Tomorrow,” Los PFLD, 20 de abril de 2007, última visita, 23 de mayo de 2014, disponible en http://episkoposcain.blog spot.ca/2007/04/hal-turner-raid-planned-for-tomorrow.html.

35 Asterix, “August Theme: Anonymous Takes Back Chanology”, Why We Protest, 14 de julio de 2008, última visita, 23 de mayo de 2014, disponible en http://whyweprotest.net/community/threads/august-theme-anonymous-takes-back-chanology.18139/página-2.

36 Why We Protest, “False Press—We Need to Deal with This Immediately”, 22 de marzo de 2008, disponible en http://whyweprotest. net/community/threads/false-press-we-need-to-deal-with-this-immediately.80242

37 “Operation Slickpubes”, Motherfuckery, 10 de enero de 2009, última visita, 23 de mayo de 2014, disponible en http://motherfuckery.org/this-is-how-a-post-looks.

38 “In 2009,NYPD Issued ‘Surveillance Request’ to ‘Identify’ Anonymous Members During Their Anti-Scientology Rally,” techdirt.com, 4 de septiembre, 2013, última visita, 11 de julio, 2014.

39 Eric Hobsbawm, “Subcultures and Primitive Rebels”, en el *Cultural Resistance Reader* (Londres y Nueva York: Verso, 2002), 136.

40 Ibid., 147

41 Tony Ortega, “Meet the Man Behind WWP, the Web Home of Anonymous and Project Chanology”, The Underground Bunker, 22 de junio de 2013, última visita, 23 de mayo de 2014, disponible en http://tonyortega.org/ 2013/06/22/meet-the-man-behind-wwp-the-web-home-of-anonymous.

42 Entrevista online con el autor.

43 Anonymous, “What the Dicks Is Marblecake adn What Do They Do?” Why We Protest, 23 de junio de 2008, última visita, 4 de julio de 2014, disponible en http://whyweprotest.net/community/threads/what-the-dicks-is-marblecake-and-what-do-they-do.16012/página13.

44 Paolo Gerbaudo, *Tweets and the Streets: Social Media and Contemporary Activism* (Londres: Pluto Press, 2012).

45 Jo Freeman, “The Tyranny of Structurelessness,” The Second Wave, vol. 2, n. 1 (1972).

46 “Operation Clambake Present: The Scientology Fair Game Policy,” Operation Clambake: Undressing the Church of Scientology, última visita, 23 de mayo de 2014, disponible en http://www.xenu.net/fairgame-e.html.

Capítulo 3. Las armas de los Geeks

47 David Leigh, “Guardian Gagged from Reporting Parliament,” the guardian.com, 12 de octubre de 2009.

48 Christian Christensen, “Collateral Murder and the After-Life of Activist Imagery,” medium.com, 14 de abril de 2014.

49 EvanHansen,“Manning-LamoChatLogsRevealed,”wired.com, 13 de julio de 2011.

50 Lamo ha declarado que, puesto que ha publicado algunos artículos, es periodista. También ha manifestado que es ministro de la Iglesia de la Vida Universal. *V*éase Luis Martínez, “Bradley Manning Accuser Adrian Lamo Takes the Stand”, 20 de diciembre de 2011, abcnews.go.com.

51 EdPilkington,“Bradley Manning’s Treatment Was Cruel and Inhuman, UN Torture Chief Rules”, theguardian.com, 12 de marzo de 2012.

52 Raffi Khatchadourian, “No Secrets,” newyorker.com, 7 de junio de 2010.

53 La conexión puede llevarse incluso mas allá, ya que el joven Julian Assange también había hecho sus propias incursiones combatiendo a la Cienciología. En Australia dirigía un proveedor de servicios de Internet de libre expresión, Suburbia, que contenía material de la Cienciología. En 1996 también organizó en Melbourne una protesta anti Cienciología.

54 Wilford’s Dog, “AMA Request Sabu from LuLSec [sic] this would be amazing,” reddit, 23 de septiembre de 2011, última visita, 29 de mayo de 2014, disponible en http://www.reddit.com/r/IAmA/comments/kpfsp/ama_request_sabu_from_lulsec_this_would_be_amazing/

55 Guest, “Untitled,” 5 de julio de 2010, última visita, 29 de mayo de 2014, disponible en http://pastebin.com/ytZ7N1x7.

56 Por razones de privacidad, no es una dirección de IP real.

57 Para más información sobre botnets, consultar el excelente trabajo de Finn Brunton *Spam: A Shadow History of the Internet* (Cambridge, MA: MIT Press, 2013).

58 “Activists Target Recording Industry Websites,” bbc.com, 20 de septiembre de 2010.

59 Ernesto, “Anti-Piracy Outfit Tries to Erase History,” torrentfreak.com, 15 de octubre de 2011.

60 David Kravets, “Wired Exclusive: I Was a Hacker for the MPAA,” abcnews.go.com, 22 de octubre de 2007.

61 Enigmax,“Anti-Piracy Outfit Threatens to DoS Uncooperative Torrent Sites,” torrentfreak.com, 5 de septiembre de 2010.

62 Enigmax, “4chan DDoS Takes Down MPAA and Anti-Piracy Websites,” torrentfreak.com, 18 de septiembre de 2010.

63 “Hackers Hit Hollywood’s Piracy Watchdog,” reuters.com, 19 de septiembre de 2010.

64 Christopher Williams, “Piracy Threats Lawyer Mocks 4chan DDoS Attack,” theregister.co.uk, 22 de septiembre de 2010.

65 Nate Anderson, “‘Straightforward Legal Blackmail’: A Tale of P2P Lawyering,” arstechnica.com, 6 de junio de 2010.

66 “Lords Hansard text for 26 Jan 201026 Jan 2010 (pt 0003),” parliament.uk, última visita, 29 de mayo, 2014, disponible en http://www.parliament.the-stationery-office.co.uk/pa/ld200910/ldhansrd/ text/100126-0003.htm.

67 Nate Anderson, “The ‘Legal Blackmail’ Business: Inside a P2P Settlement Factory,” arstechnica.com, 29 de septiembre de 2010.

68 Enigmax, “ACS:Law (Gay) Porn Letters Target Pensioners, Married Men,” torrentfreak.com, 25 de septiembre de 2010.

69 Charles Arthur, “ACS:Law and MediaCAT Close Their Doors, Ending Filesharing Claims,” theguardian.com, 4 de febrero de 2011.

70 “ACS:Law Solicitor Andrew Crossley Suspended by SRA,” bbc.com, 18 de enero de 2012.

71 Josh Halliday, “ACS:Law Solicitor at Centre of Internet Piracy Row Suspended,” theguardian.com, 18 de enero de 2012.

72 Ernesto, “Behind the Scenes at Anonymous’ Operation Payback,” torrentfreak.com, 15 de noviembre de 2010.

73 “Anonymous Is Not Unanimous,” última visita, 29 de mayo de 2014, disponible en http://pastebin.com/4vprKdXH.

74 “PPi Ask Anonymous to Stop Payback,” The pp.international.general, noviembre, 2010, última visita, 29 de mayo de 2014, disponible en http://lists.pirateweb.net/pipermail/pp.international.general/2010-November/ thread.html#8046.

75 Pirate Parties of the UK and US, “Pirate Party Op,” 19 de noviembre de 2010, última visita, 29 de mayo, 2014, disponible en http://www.scribd.com/ doc/43400303/Pirate-Party-OP.

76 Ernesto, “Behind the Scenes at Anonymous’ Operation Payback.”

77 Entrevista online con la autora.

78 Ibid.

79 Para un ejemplo, consultar “Untitled”, 24 de febrero de 2011, última visita, 29 de mayo de 2014, disponible en http://pastebin.com/0Y5CkrF9.

80 Entrevista online con la autora.

81 Entrevista online con la autora.

82 “Open Letter to Pirate Parties of United States of America and United Kingdom,” 20 de noviembre 2010, última visita, 29 de mayo de 2014, disponible en http://www.pandasecurity.com/mediacenter/wp-content/uploads/ 2010/11/opopenlettertopp.pdf.

Capítulo 4. El disparo que resonó en todo el mundo

83 Art Keller, “Dozens (Yes, Dozens) Show Up for Anonymous’ Million- Mask March,” newsweek.com, 7 de noviembre de 2013.

84 Justin Elliot, “The 10 Most Important Wikileaks Revelations,” salon. com, 29 de noviembre de 2010.

85 Martin Beckford, “Sarah Palin: Hunt WikiLeaks Founder Like al- Qaeda and Taliban Leaders,” telegraph.co.uk, 30 de noviembre de 2010.

86 Kathryn Jean López, “On This Sunday Outrage,” nationalreview.com, 28 de noviembre de 2010.

87 En esa época, los datos estadísticos estaban disponibles en http://irc.netsplit.de/networks/ top10.php and http://searchirc.com/channel-stats.

88 Richard Stallman, “The Anonymous WikiLeaks Protests Are a Mass Demo Against Control,” theguardian.com, 17 de diciembre de 2010.

89 Para disponer de cifras exactas, consultar el trabajo de Molly Sauter, *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet* (Londres: Bloomsbury Academic, 2014).

90 Noam Cohen, “Web Attackers Find a Cause in WikiLeaks,” nytimes.com, 9 de diciembre de 2010.

91 Parmy Olson, *We Are Anonymous: Inside the Hacker World of Lulz- Sec, Anonymous, and the Global Cyber Insurgency* (Nueva York: Back Bay Books, 2013), 109.

92 Sean-Paul Correll, “’Tis the Season of DDoS—WikiLeaks Edition,” PandaLabs Blog, última visita, 3 de junio 3 de 2014, disponible en http://pandal- abs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio.

93 Sean-Paul Correll, “Operation:Payback Broadens to ‘Operation Avenge Assange,’” PandaLabs

Blog, última visita, 3 de junio de 2014, disponible en http://pandalabs.pandasecurity.com/operationpayback- broadens-to-operation-avenge-assange.

94 Nick Davies, "10 Days in Sweden: The Full Allegations Against Julian Assange," theguardian.com, 17 de diciembre de 2010.

95 Michel de Certeau, *The Practice of Everyday Life*, trad. Steven Rendall (Berkeley: University of California Press, 2011), XIX.

96 Jon Snow, post en Twitter, 9 de diciembre de 2010, 5:22 hs., https://twitter.com/jonsnowC4/status/12814239458656256.

97 ZeynepTufekci,"WikiLeaks Exposes Internet's Dissent Tax,Not Nerd Supremacy," theatlantic.com, 22 de diciembre de 2010.

98 Entrevista online con la autora.

99 Mikhail Bakhtin, *The Dialogic Imagination: Four Essays* (Austin, TX: University of Texas Press Slavic Series, 1981).

100 Ethan Case, "The Dark Side of Anonymous: Everything You Never Knew About the Hacktivist Group," policymic.com, 3 de enero de 2012.

101 "Untitled", 10 de diciembre de 2010, última visita, 3 de junio 3 de 2014, disponible en http://pastebin.com/WzzJ1Jp3.

102 Joel Johnson, "What Is LOIC?" gizmodo.com, 8 de diciembre de 2010.

103 Gerry Smith, "Feds Charge 13 Members of Anonymous in 'Operation Payback' Attacks," huffingtonpost.com, 3 de octubre de 2010.

104 Para disponer de un relato definitivo sobre los primeros tiempos del activismo, consultar el trabajo de Tim Jordan y Paul Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (Nueva York: Routledge, 2004).

105 Molly Sauter, "'LOIC Will Tear Us Apart'", *American Behavioral Scientist*, 998, vol. 57 (2013): 983–100.

106 Frances Fox Piven, *Who's Afraid of Frances Fox Piven?: The Essential Writings of the Professor Glenn Beck Loves to Hate* (Nueva York: New Press, 2011).

107 Sauter, "LOIC Will Tear Us Apart."

108 Elinor Mills, "Old-time Hacktivists: Anonymous, You've Crossed the Line," cnet.com, 30 de marzo de 2012.

109 Tod Gemuese, comentario publicado en Facebook en la página de Cult of the Dead Cow, 10 de enero de 2013, última visita, 5 de junio, 2014, disponible en

http://www.facebook.com/groups/28828338908/permalink/ 10151344658883909.

110 Para disponer de un análisis extenso y esclarecedor sobre la campaña de DDoS como una intervención que amplía los objetivos del discurso pero también califica como conducta, consultar el trabajo de Sauter, *The Coming Swarm*.

111 Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, and John Palfrey, *2010 Report on Distributed Denial of Service (DDoS) Attacks*, Centro Berkman para Internet y Sociedad, 20 de diciembre de 2010, disponible en http://cyber.law.harvard.edu/publications/2010/DDoS_Independent_Media_Human_Rights.

112 Por ejemplo, en marzo de 2013, *Los Angeles Times* publicó una corrección después de haber afirmado erróneamente en un post que un cargo acusaba a Anonymous de un delito equivalente al hackeo. Consultar el trabajo de Matt Pearce, "Wisconsin Man Indicted in Anonymous Attack of Koch Industries," latimes.com, 27 de marzo de 2013. La corrección aparece cerca del final del artículo.

113 Lee Mathews, "Man Fined $183,000 for Helping Anonymous Ddos a Site for One Minute," geek.com, 10 de diciembre, 2013. Ryan J. Reilly,"Loading Koch Industries Website Too Many Times in 1 Minute Just Cost this Truck Driver $183,000," huffingtonpost.com, 2 de diciembre de 2013.

114 Sandra Laville, "Student Convicted over Anonymous Cyber-Attacks," theguardian.com, 6 de diciembre de 2012.

115 Joe Kloc, "Anonymous's PayPal 14 Enter Pleas, Most May Skirt Jail," dailydot.com, 5 de diciembre de 2013.

116 Anu Passary, "Anonymous Members Plead Guilty in Paypal DDoS Attack Case," techtimes.com, 8 de diciembre de 2013.

117 SominiSengupta,"BritishPoliceMakeArrestinNetAttacks,"nytimes.com, 28 de julio de 2011.

Capítulo 5. Anonymous en todas partes

118 Eduard Kovacs, "Anonymous Hackers Leak Documents on Governor of Italy's Lombardy Region," softpedia.com, 25 de noviembre de 2013.

119 Consultar el trabajo de Carola Frediani, *Inside Anonymous: A Journey into the World of Cyberactivism* (Informant, 2013).

120 Lina Ben Mhenni, "Tunisia: Censorship Continues as WikiLeaks Cables Make the Rounds,"

globalvoicesonline.org, 7 de diciembre de 2010.

121 QuinnNorton,“2011:TheYearAnonymousTookOnCops,Dictators and Existential Dread,” wired.com, 11 de enero de 2012.

122 IbrahimSaleh,“WikiLeaks and the Arab Spring:The Twists and Turns of Media, Culture, and Power,” *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society* (New York: Palgrave Macmillan, 2013), 237.

123 WikiLeaks, “Cable: 09TUNIS516_a,” wikileaks.org, última visita, 5 de junio, 2014, disponible en at https://www.wikileaks.org/plusd/cables/09TUNIS516_a.html.

124 John Pollock, “How Egyptian and Tunisian Youth Hacked the Arab Spring,” technologyreview.com, 23 de Agosto de 2011.

125 Véase twitter.com/TAKRIZ, última visita, 5 de junio de 2014.

126 “Tunisia Suicide Protester Mohamed Bouazizi Dies,” bbc.com, 5 de enero de 2011.

127 “Thousands of Tunisia Lawyers Strike,” aljazeera.com, 6 de enero de 2011.

128 Tarek Amara, “Tunisian Government Says Two Killed in Clashes,” reuters.com, 9 de enero de 2011.

129 Véase anonnews.org/press/item/135, última visita, 16 de junio de 2014.

130 Para consultar varios artículos representativos que presentan a Sabu como el líder, véase: Charles Arthur, “The Darkness at the Heart of Anonymous,” theguardian.com, 23 de agosto de 2011; Josh Halliday, “LulzSec Mastermind Sabu: An Elite Hacker and Star FBI Informant,” theguardian.com, 6 de marzo de 2012; Andy Greenberg, “LulzSec Leader and Informant ‘Sabu’ Let Off with Time Served,” wired.com, 27 de mayo de 2014. Para consultar artículos que presentan a Topiary como el líder, ver: Adrian Chen, “Meet the LulzSec Leader Arrested by British Police Today,” gawker.com, 27 de julio de 2011; Peter Finocchiaro, “LulzSec Leader ‘Topiary’ Arrested in Britain,” salon. com, 27 de julio de 2011.

131 John Cook and Adrian Chen, “Inside Anonymous’ Secret War Room,” gawker.com, 18 de marzo de 2011.

132 Arthur, “The Darkness at the Heart of Anonymous”.

133 Joseph Menn, “SPECIAL REPORT—U.S. Cyberwar Strategy Stokes Fear of Blowback,” reuters.com, 10 de mayo de 2013.

134 Idem.

135 Aunque tengo acceso a la mayoría del siguiente registro, no había ninguna otra mención sobre por qué no se aplicó el día cero, y cuando le pregunté a algunos de los participantes, ninguno

pudo recordar la razón. No es inusual que una cuestión o una posibilidad planteadas no se apliquen ni se vuelva a hablar nunca más de ellas.

136 Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, Filippo Menczer, “Social Phishing,” *Communications of the ACM*, (Fall 2007): 94–100.

137 “St. Jude Memorial and Virtual Wake,” The Well, 1 de agosto de 2003, última visita, 6 de julio de 2014, disponible en http://www.well.com/conf/inkwell.vue/topics/190/St-Jude-Memorial-and-Virtual-Wak-page01.html.

138 Spencer Ackerman, “Former NSA Chief Warns of Cyber-Terror Attacks if Snowden Apprehended,” theguardian.com, 6 de Agosto de 2013.

139 RyanJ.Reily, “StephenHeymann, Aaron Swartz Prosecutor, Compared Internet Activist to Rapist: MIT Report,” huf␣ngtonpost.com, 31 de julio de 2013.

140 Hal Abelson, “The Lessons of Aaron Swartz,” technologyreview.com, 4 de octubre de 2013.

141 Gabriella Coleman, “Gabriella Coleman’s Favorite News Stories of the Week,” techdirt.com, 12 de octubre de 2013.

142 Miller McPherson, Lynn Smith-Lovin, and James M. Cook, “Birds of a Feather: Homophily in Social Networks,” *Annual Review of Sociology*, Vol. 27 (2001): 415–44.

143 Roli Varma, “Why So Few Women Enroll in Computing? Gender and Ethnic Differences in Students’ Perception,” Comp*uter Science Education* vol. 20, n. 4 (2010): 301–16.

144 Para disponer de cifras más exactas, consultar el trabajo de Christina Dunbar-Hester y Gabriella Coleman, “Engendering Change? Gender Advocacy in Open Source”, 26 de junio de 2012, última visita, 9 de julio de 2014, disponible en http://culturedigitally.org/2012/06/engendering-change-gender-advocacy-in-open- source.

145 Idem.

146 Consultar el trabajo de Douglas Thomas, *Hacker Culture* (Minneapolis, MN: University of Minnesota Press, 2003).

Capítulo 6. "Moralfaggotry" en todas partes

147 BarrettBrown, post de Twiter, 9 noviembre de 2011, 21:56 h, https://twitter.com/BarrettBrownLOL/status/134464512064626689.

148 Barrett Brown, “Why the Hacks Hate Michael Hastings,” vanityfair.com, 23 de junio de 2010.

149 Ian Shapira, "'Anonymous' Movement Views Web Hijinks as Public Good, but Legality Is Opaque," washingtonpost.com, 26 de junio de 2011.

150 Richard Borshay Lee, "Eating Christmas in the Kalahari," natural historymag.com (publicado originalmente en diciembre de 1969).

151 "US Urges Restraint in Egypt, Says Government Stable," reuters.com, 25 de enero de 2011.

152 Si bien algunos Anons participan sin duda en el fraude de las tarjetas de crédito, no están en el negocio del robo a gran escala de tarjetas de crédito e identidades. Los miembros de una de las redes de fraude con tarjetas de crédito más famosas —ShadowCrew— fueron arrestados en octubre de 2004 en una acción que el periodista Kevin Poulsen ha descrito como «la mayor operación contra ladrones de identidad en la historia estadounidense». Poulsen, *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground* (Nueva York: Broadway Books, 2012), 113.

153 Para un relato definitivo de la Operación Sundevil, consultar la obra de Bruce Sterling's*The Hacker Crackdown: Law and Disorder on the Electronic Frontier*(1992), disponible en http://www.mit.edu/hacker/hacker.html.

154 "Document Management in the FBI," cap. 2 en *An Investigation of the Belated Production of Documents in the Oklahoma City Bombing Case*", Departamento de Justicia de Estados Unidos, 19 de marzo de 2002, última visita, 16 de junio de 2014, disponible en http://www.justice.gov/oig/special/0203/chapter2.htm.

155 Puesto que la FD-302 proporciona un resumen de un interrogatorio en lugar de una transcripción, activistas y abogados la han criticado durante mucho tiempo por su parcialidad. El abogado de las libertades civiles Harvey Silverglate resumió sus problemas en un artículo: "Las atemorizadas y confusas personas interrogadas, que, si niegan haber dicho lo que cualquier informe 302 afirma que dijeron, pueden ser acusadas de hacer declaraciones falsas" (Silvergate, "Unrecorded Testimony," bostonglobe.com, 11 de mayo de 2013). En mayo de 2014, el FBI cambió su política y ahora exigirá que se grabe la mayoría de los interrogatorios a sospechosos federales. (Andrew Grossman, "FBI to Record Most Interrogations of Suspects in Federal Custody,"online.wsj.com, 21 de mayo de 2014).

Capítulo 7. La venganza del Lulz

156 Jules Boykoff, *The Suppression of Dissent: How the State and Mass Media Squelch USAmerican Social Movements* (Nueva York: Routledge, 2006), 121.

157 Idem., 115–17.

158 Idem., 118.

159 Comité del Senado estadounidense para estudiar las operaciones del gobierno con respecto a las actividades de inteligencia, "COINTELPRO: The FBI's Covert Action Programs Against American Citizens," 23 de abril de 1976, última visita, 18 de junio de 2014, disponible enhttp://terrasol.home.igc.org/HooverPlan. htm.

160 Citado en "The FBI, COINTELPRO, and the Most Important Robbery You've Never Heard Of," Privacy SOS, 3 de abril de 2013, última visita 18 de junio de 2014, disponible en https://www.privacysos.org/node/1015.

161 Mark Mazzetti, "Burglars Who Took on F.B.I. Abandon Shadows," nytimes.com, 7 de enero de 2014.

162 Glenn Greenwald, "The Leaked Campaign to Attack Wikileaks and Its Supporters," salon.com, 11 de febrero de 2011.

163 Nelson D. Schwartz, "Facing Threat from WikiLeaks, Bank Plays Defense," nytimes.com, 2 de enero de 2011.

164 Consultar el trabajo de Eric Lipton y Charlie Savage, "Hackers Reveal Offers to Spy on Corporate Rivals", nytimes.com, 11 de febrero de 2011.

165 Marcus Kabel, "Ark. Court Says Wal-Mart Can Copy Data of Fired Worker," utsandiego.com, 13 de abril de 2007.

166 Gary Ruskin, "Spooky Business: Corporate Espionage Against Nonprofit Organizations," Center for Corporate Policy, 23. Disponible en http://www.corporatepolicy.org/spookybusiness.pdf.

167 Idem. El subrayado es mío.

168 Peter Bright, Nate Anderson y Jacqui Cheng, *Unmasked* (AmazonDigital Services, 2011), 54

169 Nicole Perlroth y David E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," nytimes.com, 13 de julio de 2013.

170 Ryan Gallagher, "Cyberwar's Gray Market," slate.com, 16 de enero de 2013.

171 Nate Anderson, "Black Ops: How Hbgary Wrote Backdoors for the Government," arctechnica.com, 21 de febrero de 2011.

172 Ruskin, *Spooky Business*, 3.

173 Disponible en http://pastebin.com/u4mtivNN, última visita, 17 de junio de 2014.

174 Mike Masnick, "Play by Play of How HBGary Federal Tried to Expose Anonymous ... And Got Hacked Instead," techdirt.com, 11 de febrero de 2011.

175 Joseph Menn, “Cyberactivists Warned of Arrest,” ft.com, 5 de febrero de 2011.

176 Correos electrónicos enviados en el otoño de 2010 donde se analizaba el cierre de HBGary Federal por no ser rentable y se sugería que «el puesto de Aaron Barr como director ejecutivo estaba amenazado». (Consultar la página 28 en *Unmasked* para leer los correos electrónicos donde se detalla la posición financiera de la empresa.)

177 Peter Bright, “Anonymous Speaks: The Inside Story of the HB Gary Hack,” arstechnica.com, 16 de febrero de 2011.

178 Aforismo de Karl Wilhelm Friedrich Schlegel, poeta romántico del siglo XIX (¡y súper extravagante!!!).

179 Disponible en http://archive.today/lMuqh#selection-207.17-207.32, última visita 18 de junio de 2014.

180 John Cook and Adrian Chen, “Inside Anonymous’ Secret War Room”, gawker.com, 18 de marzo de 2011.

181 Dan Kaplan, “Anonymous Takes Over Security Firm in Vengeful Hack”, scmagazine.com, 7 de febrero de 2011.

182 “Hacker of Sacramento Company HBGary Pleads Guilty”, comunicado de prensa del FBI, 6 de marzo de 2012, última visita, 18 de junio de 2014, disponible en http://www.fbi.gov/sacramento/press-releases/2012/hacker-of-sacramento-company-hbgary-pleads-guilty.

183 Parmy Olson, “Victim of Anonymous Attack Speaks Out,” forbes. com, 7 de febrero de 2011.

184 Según el plan previsto, Palantir proporcionaría su oneroso programa de análisis de enlaces funcionando en un servidor alojado, mientras que Berico «prepararía el contrato proporcionando la gestión del proyecto, los recursos para el desarrollo y el desarrollo de procesos/metodología». HBGary Federal se uniría para suministrar una «colección de inteligencia digital» y la «explotación de las redes sociales». Nate Anderson, “Spy Games: Inside the Convoluted Plot to Bring Down WikiLeaks,” arstechnica.com, 14 de febrero de 2011.

185 Parmy Olson, “Congressman Probing HBGary Scandal Fears ‘Domestic Surveillance’”, forbes.com, 23 de marzo de 2011.

186 Barrett Brown, “The Cyber-Intelligence Complex and Its Useful Idiots,” theguardian.com, 1 de julio de 2013.

187 Tim Shorrock, “US Intelligence & Outsourcing,” última visita, 17 de junio de 2014, disponible en http://timshorrock.com/?page_id=141.

188 Tim Shorrock, “Put the Spies Back Under One Roof,” nytimes.com, 17 de junio de 2013.

Capítulo 8. LulzSec

189 Steve Ragan del *Tech Herald* también se comunicó con miembros de LulzSec mientras informaba acerca de una cuestión contable técnica de los hackeos.

190 *2600*, post en Twitter, junio de 2011, 01:40hs., http://twitter.com/2600/ status/76931363755925504.

191 “A Little FAQ About Me vs. Anonymous,” Asherah Research Group, 24 de mayo de 2012, última visita, 24 de junio de 2014, disponible en http://www.back- trace- security.com/blog/844473-a-little-faq-about-me-vs-anonymous.

192 “Anonymous Message to Sony about Taking Down Playstation Network,” vídeo en YouTube, posteado por Johnny John, 22 de abril, 2011, última visita, 24 de junio de 2014, disponible en http://www.youtube.com/ watch?v=aTbLA_1nkgU.

193 “The Light It Up Contest—Geohot,” vídeo en YouTube, posteado por geohot,12 de febrero de 2011, última visita, 7 de julio de 2014, disponible en http:// www.youtube.com/watch? v=9iUvuaChDEg.

194 Cory Doctorow, “Embattled PS3 Hacker Raises Big Bank to Fight Sony”, boingboing.net, 22 de febrero de 2011.

195 Citado en el trabajo de Jason Mick, “Anonymous Engages in Sony DDoS Attacks over GeoHot PS3 Lawsuit,” dailytech.com, 4 de abril de 2011.

196 Patrick Seybold, “Update on PlayStation Network and Qriocity,” PlayStation.com, 26 de abril de 2011, última visita, 11 de julio de 2014.

197 Colin Milburn, “Long Live Play: The PlayStation Network and Technogenic Life,” en Attractive Objects: The Furniture of the Technoscientific World, editado por Bernadette Bensaude-Vincent, Sacha Loeve, Alfred Nordmann y Astrid Schwartz (Pittsburgh: PA, University of Pittsburgh Press, de próxima publicación).

198 Owen Good, “Welcome Back PSN: The Winners,” kotaku.com, 21 de mayo de 2011.

199 Paul Tassi, “Sony Pegs PSN Attack Costs at $170 Million, $3.1B Total Loss for 2011,” forbes.com, 23 de mayo de 2011.

200 “Sony Fined £250,000 After Millions of UK Gamers’ Details Compromised,” Information Commissioner’s Office, 24 de enero de 2013, última visita, 24 de junio de 2014, disponible en

http://www.ico.org.uk/news/ latest_news/2013/ico-news-release-2013.

201 “Outro,” HTP Zine 5 (2013), última visita, 24 de junio de 2014, disponible en http://www.exploit-db.com/papers/25306.

202 LulzSec, post en Twitter, 10 de mayo de 2011, 07:52hs., http://twitter.com/ LulzSec/status/68116303004708864.

203 Fotografía tomada por Alexander Sotirov. Reeditada con autorización.

204 Para disponer de una excelente historia que cubre las numerosas amenazas que acechan la seguridad en Internet, consultar el trabajo de Ronald J. Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (Toronto: Signal, 2013).

205 “Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries),” Vídeo YouTube, colgado por Joe Grand, 14 de marzo de 2011, última visita, 24 de junio de 2014, disponible en http://www.youtube.com/watch?v=VVJldn_MmMY.

206 De hecho, en 2013, un informe de seguridad calculaba que se había producido un 30 por ciento de incremento en el número total de infiltraciones comparado con 2012. Estas cifras no son incontrastables, pero aportan un sentido de la profundidad y extensión de las infiltraciones que se produjeron en un año concreto. Consultar “ITRC 2013 Breach List Tops 600 in 2013,” Centro de recursos sobre robo de identidad, 20 de febrero de 2014, última visita, 24 de junio de 2014, disponible en http://www. idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html.

207 Patrick Gray,“Why We Secretly Love LulzSec”, *RiskyBusines*s, 8 de junio de 2011, última visita, 24 de junio de 2014, disponible en http://risky.biz/lulzsec.

208 Michael Taussig, Defacement: Public Secrecy and the Labor of theNegative (Stanford: Stanford University Press, 1999), 5.

209 Véase TTI/Vanguard homepage at http://www.ttivanguard.com. Última visita, 24 de junio de 2014.

210 Dick Hebdige, *Subculture: The Meaning of Style* (Londres: Routledge, 1979).

211 Un importante productor de Hollywood adquirió recientemente los derechos cinematográficos de un artículo publicado en la revista *Rolling Stone* que relata la Operación Steubenville, una acción de Anonymous relativa a un caso de violación ocurrido en Ohio. Hasta que la película no se haya estrenado es imposible decir si distorsiona y rebaja el mensaje contracultural de Anonymous.

212 Para disponer de un análisis detallado respecto del papel que la estética y la hipérbole juegan en el pensamiento y la obra de Nietzsche, consultar el trabajo de Alexander Nehamas, *Nietzsche:*

Life as Literature (Cambridge, MA: Harvard University Press, 1987).

213 Friedrich Nietzsche, “Así habló Zaratustra” (1891), disponible en http://philosophy.eserver.org/nietzsche-zarathustra.txt (última visita, 7 de julio de 2014).

214 Walter Benjamin, *Selected Writings, Volume 1*: 1913–1926, eds. Marcus Bullock y Michael W. Jennings (Cambridge, MA: Harvard University Press, 1996), 239.

Capítulo 9. AntiSec

215 Chris Hedges, “The Revolutionaries in Our Midst,” truthdig.com, 10 de noviembre de 2013.

216 Sterling, *The Hacker Crackdown*.

217 Idem. La lista de *philes* es una entrega parcial de una más extensa en la historia de Sterling.

218 hacktivistas del mundo, uníos, “Philippine Hackers Target National Police, Demanding the Release of the Sagada 11!,” Indybay, 22 de marzo de 2006, última visita, 25 de junio de 2014, disponible en http://www.indybay.org/newsitems/2006/03/22/18099531.php. Consultar también “Electronic Civil Disobedience Journal”, *Hack This Site*, 2007, última visita, 9 de julio de 2014, disponible en http://mirror.hackthissite.org/hackthiszine/hackthis zine5.txt

219 Stuart Luman, “The Hacktivist,” chicagomag.com, 25 de junio de 2007.

220 “Operation Anti-Security”, 19 de junio de 2011, última visita, 25 de junio de 2014, disponible en http://pastebin.com/9KyA0E5v.

221 “Anti-Security: Save a Bug, Save a Life,” última visita 25 de junio de 2014, disponible en http://web.archive.org/web/20010301215117/http://anti.security.is.

222 The Lulz Boat, post en Twitter, 4 de junio de 2011, 5:34 am, http://twitter.com/LulzSec/status/76960035145650177.

223 StephenChapman, “OperationAnti-Security:LulzSecandAnonymous Target Banks and Governments,” zdnet.com, 20 de junio de 2011.

224 “Chinga La Migra Bulletin #1”, 23 de junio de 2011, última visita, 9 de julio de 2104, disponible en http://thepiratebay.se/torrent/6490796/Chinga_La_Migra.

225 “50 Days of Lulz”, 25 de junio de 2011, última visita, 25 de junio de 2014, disponible en http://pastebin.com/1znEGmHa.

226 Samantha Murphy, “Exclusive First Interview with Key LulzSec Hacker”, *New Scientist*, no. 2820 (4 de julio de 2011). Disponible en http:// www.newscientist.com/article/dn20649-

exclusive-first-interview- with-key-lulzsec-hacker.html#.U6bPdB_7Gi0. (Última visita, 26 de junio de 2014.)

227 Aldous Huxley, *Complete Essays*, (Chicago: Dee, 2000 [1934]), 526.

228 Topiary, post en Twitter, 21 de julio de 2011, 09:0hs., https://twitter.com/atopiary/status/94225773896015872.

229 Mark Schone y otros, "Exclusive: Snowden Docs Show UK Spies Attacked Anonymous, Hackers," nbcnews.com, 4 de febrero de 2014.

230 Chris Weatherhead, post en Twitter, 5 de febrero de 2014, 8:39 h, http://twitter.com/CJFWeatherhead/status/431059633071878144.

231 Transcripción, *CNN Newsroom*, 15 de agosto de 2011, última visita, 25 de junio de 2014, disponible en http://quiz.cnn.com/TRANSCRIPTS/1108/15/cnr.08.html.

232 Consultar la obra de Paolo Gerbaudo, *Tweets and the Streets: Social Media and Contemporary Activism* (Londres: Pluto Press, 2012).

233 Disponible en http://bartlulz.weebly.com. (Última visita, 25 de junio de 2014.)

234 "Disguised Member of Hacktivist Group 'Anonymous' Defends Retaliatory Action Against BART," democracynow.org, 16 de agosto de 2011.

235 "Untitled", 19 de agosto de 2011, última visita, 25 de junio de 2014, disponible en http://pastebin.com/zug52JVA.

236 "Anonymous Is Not Unanimous", 17 de agosto de 2011, última visita, 25 de junio de 2014, disponible en http://pastebin.com/4vprKdXH.

237 Consultar la obra de Chantal Mouffe, "Deliberative Democracy or Agonistic Pluralism?" *Social Research*, vol. 66, n. 3 (otoño de 1999): 745–58.

238 *BrickSquad*, vol.1, última visita, 25 de junio de 2014, disponible en thttp://download.adamas.ai/dlbase/ezines/Br1ck_Squ4d/br1ck_squ4d_vol.1.txt.

Capítulo 10. El deseo de un secreto es ser revelado

239 The Real Sabu, post en Twitter, 17 de Agosto de 2011, 4:43 h, http://twitter.com/anonymouSabu/status/103763961064865792.

240 The Real Sabu, post en Twitter, 17 de septiembre de 2011, 1:43 h, http://twitter.com/anonymousabu/status/115133670213435393.

241 The Real Sabu, post en Twitter, 17 de septiembre de 2011, 1:43 h, http://twitter.com/anonymouSabu/status/115136117925347328.

242 “USA v. Héctor ‘Sabu’ Monsegur Transcript August 15, 2011,” última visita 27 de junio de 2014, disponible en http://cryptome.org/2013/02/usa-v-monsegur-11-0815.htm.

243 Disponible en http://pastie.org/private/om3mrqvbdbmg8esddkcmw# 2-3, 347,353,365,376. (Última visita, 27 de junio de 2014.)

244 Nathan Schneider, *Thank You, Anarchy: Notes from the Occupy Apocalypse* (Berkeley: University of California Press, 2013), 28.

245 Drew Grant, “Hacker Hero ‘Weev’ Stops by Occupy Wall Street [Video]” observer.com, 21 de octubre de 2011.

246 Graham Jones, *Trade of the Tricks: Inside the Magician’s Craft* (Berkeley: University of California Press, 2011), 94.

247 Jeanne Mansfield, “Why I Was Maced at the Wall Street Protests” 26 de septiembre, 2011, última visita, 27 de junio, 2014, disponible en http://paste-bin.com/Wkckd9bR.

248 “BadCop d0x”, 26 de septiembre de 2011, última visita 27 de junio de 2014, disponible en http://pastebin.com/nC4f5uca.

249 “Anthony Bologna, Pepper Spray NYPD Officer, Transferred to Work in Staten Island,” huffingtonpost.com, 26 de octubre de 2011.

250 Karen McVeigh, “Occupy Wall Street: ‘Pepper-Spray’ Officer Named in Bush Protest Claim,” theguardian.com, 27 de septiembre de 2011.

251 “DoITT – Frequently Asked Questions: Public Pay Telephones,” NYC. gov, última visita, 27 de junio de 2014, disponible en http://www.nyc.gov/html/doitt/html/faq/payphone.shtml.

252 “Sabu / LulzSec leader”, 7 de junio de 2011, última visita, 27 de junio de 2014, disponible en http://pastebin.com/TVnGwSmG. Algunos de los detalles de este evento también procedían del fascinante perfil de Sabu hecho por Steve Fishman, “‘Hello, I Am Sabu...,’” nymag.com, 3 de junio de 2012.

253 Para encontrar críticas reflexivas sobre la dinámica de género, visitar geekfeminism.org.

254 El papel de la rareza está cuidadosamente explorado por la hacker Meredith L. Patterson en su ensayo “When Nerds Collide,” medium.com, 23 de marzo de 2014.

255 Quinn Norton, “How Antisec Died,” medium.com, 21 de noviembre de 2013.

256 Schneider, *Thank You, Anarchy*, 76.

257 “FBI Documents Reveal Secret Nationwide Occupy Monitoring,” Partnership for Civil Justice

Fund, 22 de diciembre de 2012, última visita, 27 de junio de 2014, disponible en http://www.justiceonline.org/commentary/fbi- ␣les-ows.html.

258 Colin Moynihan, “Officials Cast Wide Net in Monitoring Occupy Protests,” nytimes.com, 23 de mayo de 2014.

259 David Hume, *A Treatise of Human Nature*, eds. David Fate Norton y Mary J. Norton (Oxford: Oxford University Press, 2000), 204.

Capítulo 11. El Sabutaje

260 http://ulrikbrask.dk/operation-m4yh3m, última visita, 5 de julio de 2014.

261 Idem.

262 The Real Sabu, post en Twitter, 24 de diciembre de 2011, 2:49 pm, http://twitter.com/anonymouSabu/status/150664330763964416.

263 El comité invisible, *The Coming Insurrection* (2007), última visita, 9 de julio de 2014, disponible en http://tarnac9.wordpress.com/texts/the-coming-insurrection/.

264 “Operation m4yh3m,” última visita, 9 de julio de 2014, disponible en http:// ulrikbrask.dk/operation-m4yh3m.

265 Ibid., 25 de diciembre de 2011, 15:54 h, http://twitter.com/anonymouSabu/status/151043065501593601.

266 Ibid., 25 de diciembre de 2011, 2011, 16:57 h, http://twitter.com/anonymouSabu/status/151059108353683456.

267 “Press Release: Stratfor Hack NOT Anonymous”, 25 de diciembre de 2011, última visita, 30 de junio de 2014, disponible en http://pastebin.com/8yrwyNkt.

268 Kevin Poulsen, “WikiLeaks Volunteer Was a Paid Informant for theFBI”, wired.com, 27 de junio de 2013.

269 Para disponer de una lista completa de sitios participantes, visitarsopastrike.com.

270 Chenda Ngak, “SOPA and PIPA Internet Blackout Aftermath, Staggering Numbers,” cbsnews.com, 19 de diciembre de 2012.

271 Victoria Espinel, Aneesh Chopra y Howard Schmidt, “Combating Online Piracy While Protecting an Open and Innovative Internet,” We the People: Your Voice in Our Government, última visita, 1 de julio de 2014, disponible en

http://petitions.whitehouse.gov/response/combating-online-piracy-while-protecting open-and-innovative-internet.

272 Greg Sandoval, “New Zealand PM Apologizes to Kim Dotcom; Case Unraveling,” cnet.com, 27 de septiembre de 2012.

273 Max Fisher, “Stratfor Is a Joke and So Is Wikileaks for Taking It Seriously,” theatlantic.com, 27 de febrero de 2012.

274 “Re: Wiki Hackers Talk to The Economist,” Global Intelligence Files, 28 de marzo de 2013, última visita, 1 de julio de 2014, disponible en http:// wikileaks.org/gifiles/docs/10/1075390_re-wiki-hackers-talk-to-the- economist-.html.

275 SteveHorn, “HowtoWintheMediaWarAgainstGrassrootsActivists: Stratfor’s Strategies,” mintpressnews.com, 29 de julio de 2013.

276 Comunicación con la autora a través del correo electrónico.

277 Gary Ruskin, *Spooky Business: Corporate Espionage Against Nonprofit Organizations, Center for Corporate Policy*, 34. Disponible en http://www.corporatepolicy.org/spookybusiness.pdf.

278 “Stratfor Statement on Wikileaks”, digitaljournal.com, 27 de febrero de 2012.

279 The Real Sabu, post en Twitter, 3 de febrero de 2012, 22:22 h, http://twitter.com/anonymouSabu/status/165636278770077697.

280 Jana Winter, “EXCLUSIVE: Inside LulzSec, a Mastermind Turns on His Minions”, foxnews.com, 6 de marzo de 2012.

281 The Real Sabu, post de Twitter, 16 de agosto de 2011, 8:22 h, http://twitter.com/anonymousabu/status/103456479964700672.

282 Nigel Parry, “Sacrificing Stratfor: How the FBI Waited Three Weeks to Close the Stable Door”, Nigel Parry.com, 25 de marzo de 2012, última visita, 2 de julio de 2014, disponible en http://www.nigelparry.com/news/ sacrificing-stratfor.shtml.

283 Jana Winter, “EXCLUSIVE: Inside LulzSec, a Mastermind Turns on His Minions”.

284 George Friedman, “The Hack on Stratfor”, Stratfor.com, 11 de enero de 2012, última visita, 1 de julio de 2014, disponible en http://www.stratfor.com/weekly/hack-stratfor.

285 Nicole Perlroth, “Inside the Stratfor Attack”, nytimes.com, 12 de marzo de 2012.

286 Dell Cameron, “How an FBI Informant Orchestrated the Stratfor Hack”, dailydot.com, 5 de junio de 2014.

287 “Sentenced to 10 Years in Prison, Jeremy Hammond Uses Allocution to Give Consequential Statement Highlighting Global Criminal Exploits by FBI Handlers”, sparrowmedia.net, 15 de

noviembre de 2013.

288 Mark Mazzetti, “FBI Informant Is Tied to Cyberattacks Abroad”, nytimes, 23 de abril de 2014.

289 Daniel Stuckey y Andrew Blake, “Exclusive: How FBI Informant Sabu Helped Anonymous Hack Brazil”, motherboard.vice.com, 5 de junio de 2014.

290 Alexandra Natapoff, *Snitching: Criminal Informants and the Erosion of American Justice* (Nueva York: NYU Press, 2011), 44.

291 Lee Romney, “Pressured to Name Names”, latimes.com, 7 de Agosto de 2006.

292 Adam Goldman, “Lawsuit Alleges FBI Is Using No-Fly List to Force Muslims to Become Informants”, washingtonpost.com, 22 de abril de 2014.

293 “Notes on Sabu Arrest”, Errata Security, 6 de marzo de 2013, última visita, 1 de julio de 2014, disponible en http://blog.erratasec.com/2012/03/notes-on-sabu-arrest.html#.U64Kjx_7Gb8.

294 Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (Nueva York: Back Bay Books, 2013), 400.

295 John Leyden, “Sabu Wasn’t the Only FBI Mole in LulzSec, Suggest Leaked Docs”, theregister.co.uk, 10 de enero de 2014.

296 Ruth Rosen, *The World Split Open: How the Modern Women’s Movement Changed America*, Revised Edition (Nueva York: Penguin, 2006), 281.

297 Brian Todd and Kevin Bohn, “Computers of Obama, McCain Campaigns Hacked”, cnn.com, 6 de noviembre de 2008.

298 Entrevista online con la autora.

299 “Quebec Human Rights Commission Slams Bill 78”, cbc.ca, 19 de julio de 2012, última visita, 2 de julio de 2014, disponible en cbc.ca, 19 de julio de 2012.

300 AnonOpsIndia, post en Twitter, 17 de mayo de 2012, 6:08 am, http://twitter.com/opindia_revenge/status/203079500983050240.

301 “Official Statement from Family and Partner of Aaron Swartz,” RememberAaronSw.com, 12 de enero de 2013, última visita 2 de julio de 2014, disponible en rememberaaronsw.com/memories.

302 “Anonymous Operation Last Resort”, vídeo en YouTube, posteado por Aarons ArkAngel, 26 de enero de 2013, última visita, 7 de julio de 2014, disponible en http://www.youtube.com/watch?v=WaPni5O2YyI&feature= youtu.be.

303 Jason Howerton, “Disturbing Vídeo Leaked of Ohio High School Students Joking About Alleged Gang Rape”, theblaze.com, 2 de enero de 2013.

304 DavidKushner, “Anonymousvs.Steubenville”, rollingstone.com, 27 de noviembre de 2013.

305 Trip Gabriel, “Inquiry in Cover-Up of Ohio Rape Yields Indictment of Four Adults”, nytimes.com, 25 de noviembre de 2013.

306 “#OpJustice4Rehtaeh Statement Anonymous,” vídeo de YouTube, publicado por Anonymous Canadá, última visita, 9 de julio de 2014, disponible en http:// www.youtube.com/watch?v=7_D_zvizzKA.

307 Citado en la obra de Emily Bazelon, “Non-Consensual Sexting Leads to Child Pornography Charges for Two Men in Rehtaeh Parsons Case”, salon.com, 8 de Agosto de 2013.

308 Idem.

309 Peggy Lowe y Monica Sandreczki, “Why Was the Maryville Rape Case Dropped?” kcur.org, 11 de julio de 2013.

310 Ariel Levy, “Trial by Twitter”, newyorker.com, 5 de Agosto de 2013.

311 “Is Maryville the Next Steubenville?” Huffington Post Live, 16 de octubre de 2013, última visita, 1 de julio de 2014, disponible en http://live.huffington post.com/r/segment/is-maryville-the-next-steubenville/525d71012b8c 2a4a3d0000d2.

312 Emily Bazelon, “The Online Avengers,” nytimes.com, 15 de enero de 2014.

313 La discusión fue provocada por el comentario publicado de Larisa Mann sobre un tema similar. Mann, “What Can Feminism Learn from New Media?”, *Communication and Critical/Cultural Studies* (Verano de 2014): 1–5.

314 Stephen Duncombe, *Dream: Re-imagining Progressive Politics in an Age of Fantasy* (Nueva York: New Press, 2007).

Conclusión: El Aurora

315 Lauren Cornell, “Primary Documents” (entrevista con Laura Poitras), *Mouse Magazine*, Nº 40, última visita 7 de julio de 2014, disponible en http://www.moussemagazine.it/articolo.mm?id=1020.

316 Barton Gellman y Julie Tate, “In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are”, washingtonpost. com, 5 de julio de 2014.

317 James Risen y Laura Poitras, “N.S.A. Report Outlined Goals for More Power”, nytimes.com, 22 de noviembre de 2013.

318 Samuel Warren y Louis Brandeis, “The Right to Privacy”, Harvard Law Review, vol. IV, no. 5 (15 de diciembre de 1890). Última visita, 2 de julio de 2014, disponible en http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

319 https://help.riseup.net/en/about-us/newsletter/2013/08.

320 Jennifer Granick, “My Dinner with NSA Director Keith Alexander”, forbes.com, 22 de Agosto de 2013.

321 Consultar especialmente los trabajos de Will Potter, *Green Is the New Red: An Insider’s Account of a Social Movement Under Siege* (San Francisco: City Lights Publishers, 2011), y Arun Kundnani, *The Muslims Are Coming!: Islamophobia, Extremism, and the Domestic War on Terror* (Nueva York: Verso, 2014).

322 Muslim American Civil Liberties Coalition, Creating Law Enforcement Accountability & Responsibility (CLEAR) y Asian American Legal Defense and Education Fund (AALDEF), *Mapping Muslims: NYPD Spying and Its Impact on American Muslims* (2013). Última visita, 2 de julio de 2014, disponible en http://aaldef.org/press-releases/press-release/new-report-launched-nypd-spyings-impact-on-american-muslims.html.

323 Tim Cushing, “Former FBI Agent: NYPD’s Muslim-Spying Demographics Unit Was Almost Completely Useless”, techdirt.com, 28 de abril de 2014.

324 *Mapping Muslims*, 55.

325 Glenn Greenwald and Murtaza Hussain, “Under Surveillance”, theintercept.com, 9 de julio de 2014.

326 “Factsheet: The NYPD Muslim Surveillance Program,” ACLU, última visita 2 de julio de 2014, disponible en https://www.aclu.org/national-security/factsheet-nypd-muslim-surveillance-program.

327 Laurie Penny, “If You Live in a Surveillance State for Long Enough, You Create a Censor in Your Head”, newstatesman.com, 17 de junio de 2013.

328 Steve Lohr, “Unblinking Eyes Track Employees,” nytimes.com, 21 de junio de 2014.

329 Hace poco tiempo, dos profesores de Northwestern y Princeton examinaron aproximadamente dos mil cambios en la política a la luz de innumerables datos sobre lobistas, la élite estadounidense y las preferencias de los estadounidenses corrientes. Ambos determinaron algo que muchos ya sospechaban: «Las élites económicas y los grupos organizados que representan a los intereses comerciales tienen importantes impactos independientes en la política del gobierno de Estados Unidos, mientras que los grupos de interés populares y el ciudadano medio tienen poca o ninguna influencia independiente.» Martin Gilens y Benjamin Page, “Testing Theories of American Politics: Elites, Interest Groups, and Average Citizens”.

Perspective on Politics, de próxima publicación.

330 Eben Moglen, "Freedom in the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing", discurso pronunciado durante una reunión de la rama de Nueva York de la Internet Society, 5 de febrero de 2010. Disponible en http://www.softwarefreedom.org/events/2010/isoc-ny/ FreedomInTheCloud-transcript.html (última visita, 2 de julio de 2014). Bruce Schneier, "The US Government Has Betrayed the Internet. We Need to Take it Back," theguardian.com, 5 de septiembre de 2013.

331 Christopher Soghoian, "Protecting Privacy Can Conflict with Free Business Models", Sección 7.1 en *The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance*, tesis de doctorado, agosto de 2012.

332 Para tener información de dos libros recientes sobre políticas de los geeks, consultar los títulos publicados por Jessica L. Beyer, *Expect Us: Online Communities and Political Mobilization* (Oxford: Oxford University Press, 2014), y Patrick Burkhart, *Pirate Politics: The New Information Policy Contests* (Cambridge, MA: MIT Press, 2014).

333 Trevor Timm, "Congress Wants NSA Reform After All. Obama and the Senate Need to Pass It," theguardian.com, 20 de junio de 2014.

334 Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books, 2014).

335 "Cyber Security in the Post-Snowden Era", panel en la Conferencia de Ottawa sobre Defesa y Seguridad en 2014. Vídeo disponible en http://www. cpac.ca/en/programs/public-record/episodes/31366144 (última visita 2 de julio de 2014).

336 Véase el sitio web de Reset the Net at resetthenet.org.

337 Citado en el trabajo de Derek Mead, "'The Bottom Line Is That Encryption Does Work': Edward Snowden at SXSW," motherboard.vice.com, 10 de marzo, 2014.

338 "On the FBI Raid", 7 de marzo de 2012, última visita, 8 de julio de 2014, http:// pastebin.com/vZEteA3C.

339 "Why I'm Going to Destroy FBI Agent Robert Smith Part Three Revenge of the Lithe", vídeo en YouTube, colgado por Grenalio Kristian Perdana Siahaan, 25 de noviembre de 2012, última visita, 3 de julio de 2014, disponible en http://www.youtube.com/watch?v=VcMHdfvnEk4.

340 Adrian Chen, "Former Anonymous Spokesman Barrett Brown Indicted for Sharing a Link to Stolen Credit Card Data," gawker.com, 7 de diciembre de 2012.

341 Kevin M. Gallagher, "Barrett Brown, Political Prisoner of the Information Revolution", theguardian.com, 13 de julio de 2013.

342 Douglas Thomas, *Hacker Culture* (Minneapolis, MN: University of Minnesota Press, 2003), 241.

343 Your Anonymous News, post en Twitter, 27 de mayo de 2014, 10:53hs, https://twitter.com/YourAnonNews/status/471318266255011840

344 Jeremy Hammond, “Jeremy Hammond Reacts to Héctor Monsegur’s ‘Sentencing’: Rejects the NSA White Hat Sabu Ideology”, posteado el 2 de junio de 2014, última visita, 9 de julio de 2014.

345 Danilyn Rutherford, “Kinky Empiricism”, *Cultural Anthropology*, vol. 27, n. 3 (Agosto de 2012): 465–79.

346 Anonymous, post en Twitter, 12 de mayo de 2014, 11:52 am, http://twitter.com/blackplans/status/465897377468260352.

347 Me gustaría dar las gracias a Scott Kushner por señalar la sutil pero importante diferencia que existe entre la falta de voluntad para reconocer la naturaleza política de una acción frente a la deslegitimación que se lleva a cabo precisamente porque se percibe la acción como un hecho políticamente potente.

348 Jane Bennett, *The Enchantment of Modern Life: Attachments, Crossings, and Ethics* (Princeton, NJ: Princeton University Press, 2001), 4.

349 Ernst Bloch, *The Principle of Hope*, Vol. 1, (Cambridge MA: MIT Press, 1995), 3.

350 Idem. 5.

351 Whitney Phillips, *This Is Why We Can’t Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture* (Cambridge, MA: MIT Press, de próxima publicación en 2015).

352 David Foster Wallace, “E Unibus Pluram: Television and U.S.Fiction”, *Review of Contemporary Fiction*, vol. 13, no. 2: 151–94.

353 “Waiting for the Tsunami - Bifo”, vídeo en YouTube, posteado por alterazi- onivídeo alterazionivideo, 29 de agosto, 2007, última visita 8 de julio de 2014, disponible en http://www.youtube.com/watch?v=5eojG4Hom3A#t=10.

354 Por supuesto, debido a la enorme pluralidad exhibida en las sociedades industriales contemporáneas, es ingenuo y peligroso reducir algo tan complejo como los sentimientos políticos a simples “estructuras de sentimiento”, tomando prestada la acertada frase de Raymond Williams. Sería igualmente ingenuo descartar completamente un análisis de las tendencias dominantes —ya sean económicas o afectivas— tales como el giro hacia el cinismo. Raymond Williams, *Marxism and Literature* (Oxford: Oxford University Paperback,

1978).

355 Plan C/The Institute for Precarious Consciousness, “We Are All Very Anxious,” última visita 9 de julio de 2014, disponible en http://www.weareplanc.org/we-are-all-very-anxious.

356 Bloch, *The Principle of Hope*, Vol. 1, 5.

357 Richard Sennett, *Together: The Rituals, Pleasures and Politics of Cooperation* (New Haven, CT: Yale University Press, 2012), 242.

Epílogo: El estado de Anonymous

358 Frank Bajak, “Top South American Hackers Rattle Peru’s Cabinet”,bigstory.ap.org, 2 de septiembre de 2014.

359 Consultar la página de inicio de Gamma Group en https://www.gammagroup.com/, última visita, 21 de julio de 2015.

360 WikiLeaks, “The Spy Files: GAMMA FINFISHER TROJAN,” wikileaks.org, última visita, 21 de julio de 2015, disponible en https://wikileaks.org/ spyfiles/list/tags/gamma-finnfisher-trojan.html.

361 Morgan Marquis-Boire y Bill Marczak, *From Bahrain With Love: FinFisher’s Spy Kit Exposed?*, The Citizen Lab, 25 de julio de 2012, disponible en https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers- spy-kit-exposed/. Aunque los investigadores no pudieron confirmar que fuese el gobierno quien envió el programa de software, es sospechoso que los datos capturados se enviaran a una dirección de IP en Bahrein. Para el desmentido de Gamma, consultar el artículo de Vernon Silver, “Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy”, bloomberg.com, 27 de julio de 2012.

362 Cora Currier y Morgan Marquis-Boire, “Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters,” firstlook. org/theintercept, 7 de agosto de 2014.

363 “HackBack”,n.d.,lastaccessedJuly21,2015,availableathttp://0x27.me/HackBack/0x00.txt.

364 Idem.

365 Cora Currier y Morgan Marquis-Boire, “Leaked Documents Show FBI, DEA and US Army Buying Italian Spyware,” firstlook.org/thein-tercept, 6 de julio de 2015.

366 Hacked Team, post en Twitter, 5 de julio de 2015, 5:26 h, disponible en http://core0.staticworld.net/images/article/2015/07/hackingteam_1- 100594937-orig.jpg, última visita, 21 de julio de 2015.

367 Phineas Fisher, post en Twitter, 5 de julio, 2015, 11:04 h, https://twitter.com/GammaGroupPR/status/617937092497178624.

368 Anon2World, post en Twitter, 25 de junio de 2015, 8:48 h, https://twitter.com/Anon2earth/status/614279036278284288.

369 Steven Chase, “Cyberattack Deals Crippling Blow to Canadian Government Websites,” theglobeandmail.com, 17 de junio de 2015.

370 Consultar la transcripción del periodista de los procedimientos que se llevaron a cabo el jueves 22 de enero de 2015, disponible en https://pdf.yt/d/0SWY7AoPOoovRD_a, última visita, 21 de julio de 2015.

371 Idem.

372 Quinn Norton, “We Should All Step Back from Security Journalism”, medium.com, 23 de enero de 2015.

373 Disponible en http://freelauri.com/, última visita, 21 de julio de 2015.

374 Tor, “Interview with Tor Summer of Privacy Student Donncha O’Cearbhaill,” última visita, 21 de julio de 2015, disponible en https:// blog.torproject.org/blog/interview-tor-summer-privacy-student- donncha-ocearbhaill.

375 Consultar por ejemplo el trabajo de Lee Rainie y Mary Madden, *Americans’ Privacy Strategies Post-Snowden*, Pew Research Center, 16 de marzo de 2015, disponible en http://www.pewinternet.org/2015/03/16/americans- privacy-strategies-post-snowden/.

376 James B. Comey, “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?,” speech given at Brookings Institution, 16 de octubre de 2014, última visita, 21 de julio de 2015, disponible en https:// www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and- public-safety-on-a-collision-course.

377 Helen Nissenbaum, “The Meaning of Anonymity in an Information Age,” *Information Society*, vol. 15, no 2 (Mayo den1999): 141–4.

378 Disponible en https://thepaypal14.com/story-keth.htm, última visita, 21 de julio de 2015.

379 Consultar https://twitter.com/ro0ted, última visita, 23 de julio de 2015.

380 Consultar la corrección incluida al final del artículo de Matthew Braga, “Anonymous Claims It Leaked Passwords and Credit Card Info of Canadian Officials,” motherboard.vice.com, 23 de junio de 2015.

381 Peter Sterne, “Gawker in the Fight of Its Life with Hulk Hogan Sex-Tape Suit”, capitalnewyork.com, 12 de junio de 2015.

382 Editores, “*Newsweek’s* Statement on the Bitcoin Story”, newsweek.com, 7 de marzo de 2014.

383 Si bien aparentemente no han seguido adelante con la presentación de una demanda, algunos partidarios de Bitcoin organizaron una campaña de recaudación de fondos colaborativa para ayudar a financiar a Nakamoto y consiguieron reunir aproximadamente el equivalente a 14.000 dólares en Bitcoin. Consultar el vídeo en YouTube “Dorian Nakamoto—Thank You, Bitcoin Community”, posteado por aantonop, 22 de abril, 2014, última visita 23 de julio de 2015, disponible en https://www.youtube.com/ watch?v=w7YmJZ-qVW8.

384 Julian Assange, “Assange: How ‘The Guardian’ Milked Edward Snowden’s Story”, newsweek.com, 20 de abril de 2015.

385 Siobhan Gorman, “Alert on Hacker Power Play”, wsj.com, 21 de febrero de 2012.

386 Para consultar la diatriba de Twitter, visitar este hilo. Anonymous, post en Twitter, 14 de Agosto de 2014, 08:14hs., https://twitter.com/Crypt0nymous/status/ 499937201825001472.

387 Jack Bratich, “Popular Secrecy and Occultural Studies”, *Cultural Studies*, vol. 21, n. 1 (enero de 2007): 42–58.

388 Consultar también el trabajo de Clare Birchall, “Transparency, Interrupted: Secrets of the Left”, *Theory, Culture and Society*, vol. 28, n. 7/8 (diciembre de 2011): 60–84.

389 Para disponer de un análisis antropológico de la insidiosa lógica contemporánea que caracteriza al secretismo de estado en Estados Unidos, consultar el trabajo de Joseph Masco, *The Theater of Operations: National Security Affect from the Cold War to the War on Terror* (Durham, NC: Duke University Press, 2014).

390 Julian Assange y otros, *Cypherpunks: Freedom and the Future of the Internet* (Nueva York: OR Books, 2012), 5.

391 Consultar especialmente el trabajo de DarinBarney, “Publics without Politics: Surplus Publicity as Depoliticization”, en *Publicity and the Canadian State: Critical Communications Perspectives*, ed. Kirsten Kozolanka (Toronto: University of Toronto Press, 2014), 70–86.

392 Robin Celikates, “Civil Disobedience as a Practice of Civic Freedom”, en *On Global Citizenship: James Tully in Dialogue*, series ed. David Owen (Nueva York: Bloomsbury, 2014), 223.

393 Ewen MacAskill, “Second Leaker in US Intelligence, Says Glenn Greenwald,” theguardian.com, 11 de octubre de 2014.

394 Consultar el trabajo de Fruzsina Eördögh, “How Big Is Anonymous? Maybe Bigger than You Thought,” csmonitor.com, 8 de julio de 2015, para disponer de un artículo que cubre un estudio sociológico reciente sobre la presencia de Anonymous en Facebook que sugiere que el

conjunto de las protestas es mayor y más global de lo que se creía previamente.

395 Entrevista personal, 15 de junio de 2015.

396 Consultar el trabajo de Celia Britton, “Opacity and Transparency: Conceptions of History and Cultural Difference in the Work of Michel Butor and Edouard Glissant,” *French Studies*, vol. 49, n. 3 (julio de 1995): 308–20.